PhD Thesis

Digital Forensics Practices: A Road Map for Building Digital Forensics Capability

Ahmed Jasim Almarzooqi

A Doctoral Thesis Submitted in Partial Fulfilment of the Award of Doctor of Philosophy

Faculty of Technology
De Montfort University
Leicester, United Kingdome

1st November, 2016

Abstract

Identifying the needs for building and managing Digital Forensics Capability (DFC) are important because these can help organisations to stay abreast of criminal's activities and challenging pace of technological advancement. The field of Digital Forensics (DF) is witnessing rapid development in investigation procedures, tools used, and the types of digital evidence. However, several research publications confirm that a unified standard for building and managing DF capability does not exit. Therefore, this thesis identifies, documents, and analyses existing DF frameworks and the attitudes of organisations for establishing the DF team, staffing and training, acquiring and employing effective tools in practice and establishing effective procedures.

First, this thesis looks into the existing practices in the DF community for carrying out digital investigations and more importantly the precise steps taken for setting up the laboratories. Second, the thesis focuses on research data collected from organisations in the United Kingdom and the United Arab Emirates and based on this collection a framework has been developed to understand better the building and managing the capabilities of the DFOs (DFOs). This framework has been developed by applying Grounded Theory as a systematic and comprehensive qualitative methodology in the emerging field of DF research. This thesis, furthermore, provides a systematic guideline to describe the procedures and techniques of using grounded theory in DF research by applying three Grounded Theory coding methods (open, axial, and selective coding) which have been used in this thesis. Also the techniques presented in this thesis provide a thorough critique, making it a valuable contribution to the discussion of methods of analysis in the field of DF.

Finally, the thesis proposes a framework in the form of an equation for analysing the capability of DFOs. The proposed framework, called the Digital Forensics Organisation Core Capability Framework, offers an explanation of the factors involved in establishing the capability for a digital forensics organisation. Also software was developed for applying the framework in real life.

Acknowledgement

I thank **Allah (God)** for giving me strength to complete this research.

I also would like to express my thanks to several people for their support and guidance during this research. I would like to express my appreciation to my supervisor **Dr Andy Jones** for his guidance, commitment, for tolerantly reading my draft chapters and thesis, and encouragement to publish papers.

I would also like to thank **Dr Richard Howley**, my second supervisor and **Dr Helge Janicke,** my course advisor for their guidance, advice and constructive criticism especially in the beginning of my PhD journey.

My thanks also go to all the participants of this research for their kindness and co-operation, academics, particularly **Dr Shamim Ahmad** and **Professor Rafael Brown,** the support staff and colleagues in the Department of Technology, De Montfort University, Leicester.

Finally, I would like to thank Dubai Police for providing me scholarship to pursue my studies at De Montfort University, Leicester, UK, particularly Deputy Chief of Police and General Security, **LT.General Dhahi Khalfan** for his continuous encouragement to gain knowledge. Also my cordial gratitude goes to, Late **LT.General Khamis Al Muzainah,** Commissioner Dubai Police for providing me the opportunity to obtain my higher degree, who very sadly passed away during this research. Cordial thanks also go to the Director of Digital Forensics, **LT.Colonel Rashid Lootah** for his ideas and support in this study.

Dedication

This work is dedicated to my parents who encouraged and supported me all through my study, words and enduring love, particularly of my mother who provided me the real motivation for completing my higher studies.

The work is also dedicated to my brothers and sister who remained a constant source of encouragement and support throughout my life.

Finally, my thanks are extended to my friends for their continuous support all through my study period.

Declaration and Publications

I declare that, to the best of my knowledge, no portion of the work referred to in this thesis has been submitted in support of an application for another degree, or qualification, to any other university, or institute of learning. Some of the material contained here has been presented in the form of the following: (cf. Appendix 6)

Professional Conference Papers (Published):

1. Almarzooqi, A. and Jones, A., 2016, January. A Framework for Assessing the Core Capabilities of a Digital Forensic Organization. In *IFIP International Conference on Digital Forensics* (pp. 47-65). Springer International Publishing

2. Almarzooqi, A., Jones, A. and Howley, R, 2016 May. APPLYING GROUNDED THEORY METHODS TO DIGITAL FORENSICS RESEARCH. In *the 11th Annual ADFSL conference on Digital Forensics, Security and Law.*

Professional Conference Papers (Under Review):

1. Almarzooqi, A. and Jones, A., 2016, October. Establishing Tool Testing Capability Using DFOCC. (Appendix 7)

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Meaning
ACPO	Association of Chief Police Officers
ASCLD	American Society of Crime Lab Directors
CCCI	Certified Computer Crime Investigator
CCE	Certified Computer Examiner
CEECS	Certified Electronic Evidence Collection Specialist
CFAA	Computer Fraud and Abuse Act
CFCE	Certified Forensic Computer Examiner
CFReDS	Computer Forensic Reference Data Sets
CFTT	Computer Forensic Tool Testing
CPD	Continuing Professional Development
DFOCC	Digital Forensics Organisations Core Capability
DFRWS	Digital Forensic Research Workshop
DFC	Digital Forensic Capability
DFMF	Digital Forensics Management Framework
DFO	Digital Forensic Organisation
DFR	Digital Forensics Readiness
DE	Digital Evidence
ECSI	Electronic Crime Scene Investigation
EnCE	EnCase Certified Examiner
EnCEP	The EnCase Certified eDiscovery Practitioner
DF	Digital Forensics
FR	Forensics Readiness
FRED	Forensic Recovery of Evidence Device

GT	Grounded Theory
HTCIA	High Technology Crime Investigation Association
HTCN	High-Tech Crime Network
IACIS	International Association of Computer Investigation Specialists
ICCE	International Conference on Computer Evidence
ISO	International Organisation for Standardisation
ITA	Information Technology Act
IOCE	International Organisation on Computer Evidence
NIST	National Institute of Standards and Technology
NSRL	The National Software Reference Library

Chapter One: Introduction to Research

This research explores the practices of Digital Forensics (DF), starting from fundamental procedures of laboratory establishment, selecting appropriate tools for investigation, hiring experts and the identification and provision of staff training. It is recognized that the current focus in the field of DF is on the quality of the data extraction from different media devices, which is based on the demand by organisations and governments. This thesis focuses on developing a standard framework for the creation and management of the capability in the field of DF, by establishing criteria for policy development, tool selection, hiring experts and training requirements. This research will benefit many organisations around the world to develop and manage their forensic capability and a framework for the contribution to knowledge.

Modern technology aids criminals in the exploration of new ways of committing crimes (Boniface et al 2015). It is difficult to measure accurately the rate of computer crimes because very few countries gather statistics on the subject. However, Holt (2003) conducted studies of computer crime victimization based on the Computer Emergency Response Team (CERT) of computer crimes in Australia, Canada, Japan, Malaysia, The Netherlands, South Korea, the United Kingdom (UK) and the United States of America (USA). Holt found that computer crimes are indeed on rise, especially in Canada, Australia, the UK, and the USA, are predicted that the increase is likely to continue. According to the report by PricewaterhouseCoopers (PwC) report that 32% of organisations are affected by cybercrime allowing cybercrimes to become them second most economic crimes reported (PwC, 2016)

The increasing number of cybercrimes put a pressure on organisations to implement cyber forensics tools to fight against such activities (Vanlalsiama and Jha, 2015). Many organisations spend time and money to stop such threats which are becoming harder to deal with as technology develops and its use becoming more affordable for more people. Recently the UK government, in an attempt to protect companies from cybercrimes and to

express how serious cyber threats are, urged companies and business leaders to secure their assets by following the Cyber Security Guidance for Business which was developed by the government (Paul, 2012), similarly in 2015 the USA government issued a cyber security guidance for different organisations aiming to secure the cyber space (Lemieux, 2015). Employee's misconduct and the increasing concerns over intellectual property theft are also becoming the main concerns of organisations. Data loss, including customer and proprietary data are now the second largest source items of losses (Richardson and Director, C.S.I, 2008).Recently Yahoo confirmed 500 million user accounts has been stolen from the company's network making this breach the biggest data breach in history (Lord ,2016)

Casey (2012, 2016) argues that IT security is not enough to keep organisations secure and there is need for "rethinking about IT security investment strategies considering threats, outsourcing partners and risk of data breach". When a cybercrime occurs or there is a security breach, many organisations lack proper guidelines to conduct a forensic investigation and fail to bring the investigation to a productive conclusion (Grobler, 2011; Sinangin, 2002). One of the reasons behind that is the lack of general awareness and standard practice for DFO's, which led the UK government to develop a guideline to protect their data and how to deal with cybercrimes (Paul, 2012).

Computer forensics started in early 1970's when the US Federal Rules of Evidence controlled the use of Digital Evidence (Nelson et al. 2010). The Federal Bureau of Investigation in the USA first began using computer evidence to investigate and keep the proof of criminal activity in 1984 (Baryamureeba and Tushabe, 2004). Computer forensics gradually developed from unorganized phase, which lacked clear goals, to specific tools and where there were major legal gaps (Dewald, 2015; Baryamureeba and Tushabe, 2004). It was not until in 1991, in the International Association of Computer Investigation Specialists (IACIS) conference in Portland, Oregon, that the term "Computer Forensics" was first coined (Coulondre, 2008). This item then moved to a more structural outline with tools and admissible procedures for courts. A Daubert Standard or Daubert Test branched from the USA Supreme Court's ruling in Daubert vs. Merrell Dow Pharmaceuticals (1993).

Daubert Test provided standard criteria for scientific evidence to be admissible in the court based on four main categories: Testing, Error Rate, Publication and Acceptance.

The need for computer forensics went far beyond hard disk analysis, yet remained insufficient in the rapid developing world of technology. Furthermore, digital evidence did not remain only in the form of Emails and Internet activities but they developed with the technology and became necessary in order to establish the root cause of incidents (Casey, 2016). This brief history of the development of computer forensics shows the number of challenges faced by organisations, which will be addressed in detail in Chapter 2.

This research also explores the available frameworks of DF, conducts a comparative study, and proposes a framework for developing a DFC. Furthermore, it will focus on the implementation of DF capability in order to study, record and analyse the stages and procedures taken by organisations in developing their capability. Nikkel (2006) identified the main challenges which organisations face when establishing DF capability. Grobler (2011) in addition identified the following challenges to create a DF capability and the framework for DFOs.

The next questions arise:

- Where and to whom does the DF team report?
- Typical DF readiness challenges are to establish forensic resources,
- Obtain management support and awareness.
- Formal contact channels must be established to ensure efficient communication with the forensic team, and other internal and external stakeholders.
- The forensic team should be trained so that the required skills exist to facilitate successful investigations. It is also important to acquire efficient and relevant forensic tools to conduct investigations.

Currently DF aims at acquiring evidence and to investigate incidents which require a framework and policy to govern the process. In other words, a comprehensive framework is needed for DF in an organisation that takes into account more than just specific scenarios

and which is practical (Naqvi et. al 2010; Nikkel, 2006). To do this, the framework has to be better managed, with better staffing, training, and tools.

1.1 Statement of Problem

Several research (Grobler, 2011; Grobler, Louwrens, & von Solms, 2010; Garfinkel,2010; Nikkel, 2006) shows that there is no unified standard or framework for developing, managing, and implementing DFC in organisations with proper staffing, training, education (Losavio et.al 2016; McCarrin and Garfinkel, 2014), selecting tools, management, and governance. This is discussed in more detail in section 1.4 and 2.3.

1.2 Objectives and Research Questions

This research will identify, document, and analyse existing DF frameworks and the attitudes of organisations for establishing their team, staffing and training, and acquiring and employing effective tools in practice. It will also look into various leading approaches and practices in the DF community for carrying out digital investigations and more importantly the precise steps for setting up the laboratories. Finally, it will primarily focus on research data from organisations in the UK and the UAE. Before setting out to achieve the overall goals of the research, it is important to first to propose the research questions and research objectives.

1.3 Research Aims, Objectives, Questions and Methodology

Research questions were consequence of reviewing the literature and identifying the gaps (cf. Chapter 3.1) where answers to the below questions below were not available. Few scholars recommended the need for creating a standard in specific areas of DF from which the researcher used as standing point to formulate the research questions and set the objectives. These scholars, however, did not specifically suggest questions relating to whether and how a DFO may be deemed capable, specifically taking into account staffing, policies, procedures, and tools. After identifying the gaps in the literature, the researcher developed his questions as presented below:

- What recommendations exist in the literature regarding developing DFC?

- If recommendations are available, how widely are they used?
- Is there a standard practice?

As above questions identifying available recommendations for developing DFC by reviewing existing literature, further questions developed:

- How do organisations develop their DFC?
- What guidance do organisations use to develop the DFC?
- What challenges are faced by organisations in developing their DFC?

The objective of the above questions is to find and document how a range of organisations develops their DFC. This could be achieved by conducting empirical studies of the practices in the UK and UAE through a survey, interviews, and/or visit their DF sites.

From this further questions developed:

- Is there a standard pattern identifiable in developing DFC between different organisations that can be utilised in creating a DF governance framework?
- What is the role of international and national law enforcement and judicial bodies in developing DFC?

The objective of the above questions was to identify the extent to which best practices exist in developing a DFC, mainly by looking at existing literature and by empirical studies of the practices in the UK and UAE through interviews and/or visit of the DF sites.

From this then further questions developed as follows:

- What influence do regulations and organisational, social and professional procedures have on the development of DFC?
- How do digital forensic professionals recognize and manage pressure from various stakeholders on their professional practices?

The objective of the above questions was to evaluate the impact of organisational and cultural influences in developing forensic provision and its implementation, mainly by

looking at the existing literature and by empirical studies of the practices in the UK and UAE through interviews and/or visit of their DF sites.

More questions emerged were:

- How do organisations select and validate their tools?
- What tools are used?
- How effective they are?
- How can forensic provision improve tools?

The objective of the above questions was to document the range of tools used in a variety of organisations and how the choice is made for their use, mainly by looking at existing literature and by empirical studies of the practices in the UK and UAE through a survey, interview, and/or visit of their DF sites.

Finally the two sets of questions included:

- How training needs are identified?
- How training needs are met?
- What qualifications are looked for in the forensic professional?
- How effective are professional bodies and training organisations in providing competent professionals?

The objective of the above questions was to identify and document the training requirements for different forensic practitioners in a range of organisations, practically with regard to Continuing Professional Development (CPD), mainly by looking at existing literature and by empirical study of the practices in the UK and UAE through a survey, interview, and/or visit of their DF sites.

And

- What is the structure for DFC in a range of organizations and cultures?

The objective of the above questions was to map the current provision of DF in a range of organisations and cultures.

1.4 Contribution to Knowledge

In past few years, a significant advancement occurred in knowledge gained for increasing the quality of digital evidence (Liu, 2016; Guo, et al. 2009); however, fewer contributions have been made in developing standards and criteria for computer forensics. Furthermore, efforts in the past two decades focused on data preservation and data presentation but they lack the universal strategy and advanced research (Casey, 2016; Liu, 2016 Grobler, 2011; Baryamureeba and Tushabe, 2004). There are a number of reasons behind which include, what these authors believe is the reactive response to DF, coping with rapid improvements in technology, and lack of communication among DFOs. For example, until now research materials are usually restricted to certain private organisations and governmental departments and they are not willing to share them (Garfinkel et al. 2009). The Digital Forensic Research Workshop, for example, only began bringing together scholars and practitioners in 2001 (DFRWS, 2012).

According to the National Institute of Justice in the USA (2010), for more effective and efficient results in digital investigation, standard and ideal practices must be established and conducted. Such standard or ideal practices will not only cover basic investigational steps but also will cover strategies on how organisations should establish their laboratories, select their tools, hire their staff and offer training. Many organisations and governments aim to protect themselves from cyber-attacks, but there is no clear strategy to allocate their resources in terms of establishing an efficient DFO.

This research will contribute to knowledge in three ways. (i) it will provide data on how DFOs build and manage their laboratories and organisations by identifying, documenting and analysing the stages and procedures taken (ii) the research applies grounded theory to DF research and contributes to knowledge by giving a systematic guidance on how to apply Straussian grounded theory to DF research (iii) the research will contribute to knowledge by adding a theory for building and manging DFC. The theory ultimately resulted in a

proposed framework for the developing and managing a DFO, which is generated from applying grounded theory to the data collection. The core categories that arose from the grounded theory methodology contributed to knowledge by identifying the core factors that organisations could take into account when building and managing their DFO. This research further contributes to knowledge by identifying gaps in the literature on developing and managing a DFO, and suggesting the proposed framework as a comprehensive tool for assessing organisational need in developing and managing DFO.

1.5 Organisation of the Thesis

To achieve the aims and objectives stated in section 1.3, the thesis has been organised into nine chapters as follow:

Chapter 1 provides and introduction to the research states the problems, explains research aims and objectives and contribution to knowledge.

Chapter 2 discusses the review of the literature.

Chapter 3 explains the research methodology by defining the research methodology implemented. It also provides a review of the research questions in context with current literatures. In addition, this chapter explains methods and instruments adopted in the research providing justification for the selection of each instrument and method.

Chapter 4 describes the pilot study and initial data collection design including explanation of the organisations and candidates selected for the pilot study also describes the empirical research including planning of the data collection, reviewing lessons learned from the pilot study and design of data collection in this research.

Chapter 5 describes data analysis and explains how the researcher applied grounded theory using Straussian procedures and techniques to analyse data collection.

Chapter 6 reports the outcomes of the research data.

Chapter 7 proposes a framework, which expresses the relationships among abstract concepts in DFOs.

Chapter 8 is conclusion and future work.

Chapter Two: Literature Review

2.1 Introduction

This chapter contains the literature review and it's organised as below.

The first part provides an overall review of the existing work carried out in DF, and identifies the available recommendation for its building and management DF. It also discusses Digital Forensics Readiness (DFR).

The second part identifies DF training needs and how the Digital Evidence (DE) can be influenced by training and certifications. Currently, DF does not have any recognised body for professional representation that require minimal educational requirement to become a DF professional.

The third part discusses the most commonly used DF tools and how organisations select these tools and measure their effectiveness of the DF tools. DF tools play a vital role in the process of any DF investigation. The functionality of tools has developed and become more advanced in a very rapid manner.

DF development contribution will be addressed in the fourth part from a number of perspectives to confirm that the literature lacks research in providing a complete solution in developing DFC. Furthermore in this part the author explains DF infrastructure, legalisation and procedural development of DF in detail.

The fifth part identifies organisational, social and professional influences on the development of DFC and discusses the technical and legal challenges related to DF and suggested solutions to overcome these challenges.

The above factors are important in creating DFC. This literature review examined DF infrastructure, education, tools, principles and methods, and challenges to determine ultimately, with an overview of these factors, if building a comprehensive DFC can be proposed. The author will take into account the concept of organisation structure and design

under organisational theory to analyse the DF system and the potential for creating a DFC standard that takes into account the factors mentioned above, especially the challenges to DF**.**

2.2 Background of Digital Forensics

The field of DF is witnessing frequent technological updates and challenges are on the increase; however, contributions to develop DF are mostly focused on specific areas in the field without focusing on building a DFC. DFC might be defined as the ability of implementing and managing DF in an organisation with proper staffing, training, tool selection, management, and governance.

The major contribution in the development of the field of DF has been documented and reported in the UK and the USA (Liu & Uehara, 2009). DF started to be known as a discipline approximately 30 years ago. For example, in the USA DF started as a professional and scientific discipline in mid-1980 by the Federal Agencies. This discipline was established after observing an increase in the rate of computer crimes immediately after the introduction of personal computers, which aided criminals to commit more crimes (Jones and Valli, 2011). However, the first dedicated group in the field of DF was the computer crime unit of the Metropolitan police in the UK in 1984 (Goodwin, 2003). In addition to that Association of Chief Police Officers (ACPO) was the first to produce guidelines for computer crimes investigations in 1998 (Pollitt 2001; Sommer 2011).

In other parts of the world DF started in the early 21st century (Liu & Uehara, 2009). We observe that the reason behind the fast development of DF is the substantial contribution from UK and USA scholars in this field. This helped other countries to develop DF infrastructures faster and in a more structured manner than the USA and the UK. Other reasons behind the rapid development of the DF infrastructure might be the increased spreading of technology and the need to prevent/reduce the damage caused by cybercrimes also to stop the criminals from committing cybercrimes.

DF currently does not have any recognised body for professional representation that requires minimal professional educational standard to become a DF professional.

Therefore, training in the field of DF is crucial for maintaining the competency of DF investigators (Jones and Valli, 2011). Grafinkel (2010) claims that lack of composite, genuine training programs in the field of DF is a serious problem because the materials used in training are too simple and real cases are not shared between various organisations.

As digital evidence is mainly collected by tools, the data collected this way must be reliable and legally admissible. As technology advances, the demand for DF tools increases and this encourages many vendors to produce a wide range of DF tools. As a result, the market is currently offering a wide range of DF tools by various vendors alongside open source tools and proprietary tools that have been developed within organisations and they must select the most appropriate tools for their organisations to combat cybercrime.

As technology advances, the challenges and pressure towards development and progress in the field of DF also increases. With every release of a new technology DF needs to be able to deal with such innovations technologically and legality. Over the past 30 years, DF has witnessed a number of challenges which it has dealt with successfully, while other challenges are still causing pressure and challenge to the DF development.

2.3 Digital Forensics Infrastructure

As infrastructural issues play a major role in the development of DFC, this section provides an overview of the existing work done in DF. It also discusses the available recommendations for DF development. Also discussed are the educational degrees in the field of DF around the world. Also is discussed DFR in the organisations.

2.3.1 Digital Forensic Capability Development

The National Institute of Standards and Technology (NIST) is an agency within the U.S. Department of Commerce. The goal of NIST is to encourage development by producing and enhancing measurements and technological standards to improve the economy (NIST, 2016). NIST is considered to be one of the first institutions to provide standards in the field of DF. NIST has a number of projects to enhance the field of DF. The National Software Reference Library (NSRL), Computer Forensic Tool Testing (CFTT) and Computer

Forensic Reference Data Sets (CFReDS) are examples of projects carried out at NIST and each project focuses on specific areas in DF. For example, NSRL focuses on helping DF examiners in computer system investigations, whereas CFTT is designed to test computer forensic software tools by developing tool specifications and test criteria. Finally CFRDS focuses on investigators skills development (Lyle et al. 2008).

A number of organisations were established to design, contribute and build common understanding in the field of DF. For example, IACIS was established in 1988 with members from law enforcement experts. This association is committed to contributions in the field of DF by providing education and certification to people in the field of DF (IACIS, 2016).

The International Society of Forensic Computer Examiners (ISFCE) was established to professionalize DF and provide ethical standards and conduct research in the development of DF. The first International Conference on Computer Evidence (ICCE) was held in the USA in 1993 where all the participants called for the need of more collaboration to standardize the field of electronic evidence. As a result, the International Organisation on Computer Evidence (IOCE) was officially formed two years after the first conference in 1995 (Hales, 2016; Whitcomb, 2002).

As discussed above, NIST is providing guidelines for developing the DF field in terms of tools and certifying experts. Conversely (NIST, 2016), ISFCE is providing ethical standards for DF investigations (ISFCE, 2016).

The question is ‘to what extent these standards are aiding other countries and how widely they can be used or are being used?’

2.3.2 Research in the field of Digital Forensics

DF has developed to become a dedicated academic discipline and is taught in many universities in the UK and the USA and a number of other developed countries. For example in the UK there are more than 50 postgraduate courses (MSc’s) offered, furthermore there are also a wide range of undergraduate courses and research studies in the

field of DF (UCAS, 2016; Find a masters; 2016). This author believes that the infrastructure for DF is well established in the UK and the USA, which encouraged more institutions to offer DF courses. As a result, these universities can attract many international students to get their education in the field of DF to use the knowledge gained in this subject in their countries.

On the other hand, when searching technological academic institutions in Asia, such as, India, which is considered to be one of the biggest countries in terms of population, with over a billion people and is one of the growing economic powers; although the courses offered in Indian universities in the field of DF are modest in terms of current requirement of such professionals in the market and DF research in India is still at a basal levels of development (Lallie, 2012).

Another example of the developing countries in the Middle East is the UAE, where we can find very few universities which offer degrees in the field of DF. Majority of the courses offered are at BSc and MSc levels and the content of the courses is a combination of Information Technology and DF with greater focus on security. However, the total number of courses offered in the UAE in the field of DF exist not more than 10 courses. As the UAE ranks 36th globally in cyber-crime activities and spends more than $600 million a year to fight against cyber-crimes (Preeti Kannan, 2011) this indicates that there is a need to introduce more courses, especially with DF as the main teaching (Al Obaidli and Iqbal 2011; Iqbal et. al 2013).

Education in DF lacks standard curriculum, despite the fact that there are anticipated syllabuses standards exist for DF; there is no generally accepted model (Lang et al. 2014). And the need for unifying coursers and training in the field of DF was identified by Liu (2016) as one of the areas needs to be developed.

2.3.3 Digital Forensics Readiness

DFR acts against cyber-attacks, in that it allows organisations to react through legal action under national and international laws including all precautionary measures taken (Sibiya, 2015; Mouhtaropoulos, et al. 2011). Firstly, it gives organisations the chance to prepare for

DF investigations by enforcing rules and procedures that allow staff to become familiar with the DF investigations process and requirements. As stated by Sommer (2012), *"an organization needs a management an executive framework within which crisis decisions can be made"*. Secondly, it integrates live evidence and analyses. Thirdly, it enhances the framework in organisations by using the available tools in DF investigations. Finally, it helps to find the root cause of incidents and prosecute the offenders effectively. However, many organisations are not implementing the required security policies related to DFR (Elyas et al. 2015).

In other words, DF readiness is about the preparedness of an organisation that became the victim of a digital crime or cybercrime and can handle digital evidence. DF readiness, therefore, does not address the capability of the DFO doing the investigation, rather a non-DFO that receives the services or products of a DFO. In this regard, DF readiness is not only insufficient but also not applicable to the capability of a DFO. In other words, DF readiness does not appear in the DFOCC framework because DF readiness is to a DFO client as DFOCC is to a DFO. DF readiness prepares the client while DFOCC prepares the DFO.

In this regard Grobler's (2011) emphasis is on the need for DF readiness when developing DFC in organisations. After in depth study of the current available information regarding DFC from various sources, it is suggested to be crucial to extend the creation of organisational readiness in building the DFC in the countries where needed**.**

2.3.4 Digital Forensics Management Framework

Perhaps one of the most relevant literatures about DF organisational capability is the Digital Forensics Management Framework (DFMF) which was suggested by Grobler (Bankole, 2013; Grobler, 2011). Grobler proposed the DFMF as a comprehensive approach to DF investigation. The DFMF aims at showing the multi-dimensional aspect of a comprehensive DF management framework.

Grobler and Louwrens (2006) aimed to broaden the scope of DFR by proposing what Grobler called Proactive DF or ProDF . ProDF, according to these authors, is a broader

concept than DFR. They defined ProDF as “the forensic preparation of an organisation to ensure successful, cost-effective investigation, with minimal disruption to business activities, and the use of DF to establish and manage governance programmes.”

The DFMF, however, aims mainly at a management framework and not on the DFO’s overall core capabilities. The DFMF illustrates that there is indeed a need for creating a framework to determine a DFO’s core capabilities.

2.3.5 Capability Maturity Model

The capability maturity model (CMM) has been defined as “the degree to which an organisation applies formalised processes to the management of its various business functions” Kerrigan (2013). CMM uses five levels of maturity to define the capability level of an organisation’s processes. CMM was first applied to software engineering as an assessment tool, but was later adopted in other disciplines as a framework for process improvement (González-Rojas et al. 2016; Paulk et al. 1993).

Krutz (2004) first applied CMM to computer forensics in a US Patent application. Krutz’s application of CMM to computer forensics, however, did not cover the broader discipline of DF (Kerrigan, 2013). After reviewing various DF investigation frameworks and models, Kerrigan (2013) applied CMM to DF investigations. However, while Kerrigan extended CMM to DF investigation, Kerrigan did not apply CMM to a DFO’s development and management capability. Instead, Kerrigan’s focus was on the process of investigation.

Another application of the CMM to a DFO’s capability is the model proposed by Hanaei and Rashid (2014), which is largely similar to that proposed by Kerrigan. Kerrigan, Hanaei and Rashid’s model takes into account the improvement of the process, tools (technology), and skills (people). Also like Kerrigan, Hanaei and Rashid’s model does not address a DFO’s development and management capability.

The literature, therefore, shows a trend towards the application of CMM in DF. However, there exists a gap in the literature in creating a framework for determining a DFO’s core capability. The CMM falls short in addressing a DFO’s capability because CMM is limited

to measuring processes. A DFO's capability that is not process oriented (i.e. the strength of people and policy), therefore, will not be measured by CMM.

Summary

DF research and the frameworks discussed above show that most work regarding development of DFC was contributed from the UK and the USA and some other European countries. The reason behind this is that these countries are the first to experience cyber-attacks and damage caused by cyber-criminals. In addition the governments in the UK and USA visualised and anticipated the consequences of such criminal activities and therefore, they took the initiatives to improve the field of DF by calling for conferences and standardising investigation procedures. Finally, they also provided guidelines and contributed to legislation on the practice of digital investigations which will be discussed in detail in section 2.6.

In the next section will be discussed the DF training required and certification requirements are discussed in an empirical manner. Also, the current state of the art in DF and the issues which influence DF training are also discussed.

2.4 Digital Forensics Training and Certification

Training in the field of DF is one of the most important aspects which affect the development of DFC, and training is essential to ensure the competency of the DF investigators (Losavio et.al 2016; McCarrin and Garfinkel, 2014; Jones and Valli, 2011; Grafinkel 2010; Nelson et al. 2010). This section shows how training needs are identified in DFOs and how these training needs are met. In addition this section discusses qualification and certification in the field of DF and how training and certification are important in the development of a DFC.

To identify the training needed for any DF investigator (Jones and Valli, 2011) classified three basic specialisations are required in the field of DF: acquisition, analysis and presentation. This shows that the DF investigator should have a broad understanding of technical/computer related aspects as well as legal and ethical issues with regard to DF.

2.4.1 External Influences on Training in Digital Evidence

Social and organisational issues influence the decision for determining the required training material for DF investigators. The increasing modifications in current technology and the fact that the vast majority of people are now relying on them (Bryant, 2016; Garfinkel, 2014) also affects the decision making in training in the field of DF. Because it is not logical or acceptable for a DF investigator to handle a case while he is not familiar with the media device, which is the subject of this research; for example in the USA if any case requires presentation of scientific evidence the courts asks for an expert by knowledge, skill or experience to testify or give an opinion under the 702 of the Federal rules of Evidence (Valjarevic, A. and Venter, 2012)

Therefore DF investigators must acquire the requisite knowledge of the latest technology and media devices available in the market. The amount of digital evidence that can be found on different devices is valuable to any investigation and requires fully trained DF investigators to handle the cases (Bhosale et al. 2016; Phillips and Nance 2010).

There are calls from members of the judicial system for ensuring the quality of scientific evidence used in courts to force the DF experts to be licensed (Poisel and Tjoa 2011; Phillips and Nance 2010; Meyers and Rogers 2004). This is a very important call, also is challenging in the field of DF. The use of computers and the internet is continuously increasing because their affordability and a wide range of high speed internet service providers, more social websites, and more entertainment, which normally results in more time spent by users on the internet use. Therefore, if we need to validate DE, then there are a number of factors that need to be addressed, including, to name but a few, increases in the sizes of hard disks, cloud computing, the development of new operating systems, and the advancement of internet browsers (Bryant, 2016; Sommer, 2010).

2.4.2 Current status of Training and Certification in Digital Forensics

There are number of academic institutions around the world offering undergraduate and postgraduate degrees in DF (cf.2.3.2). The current state of DF certification shows that there

are many certifications and training programs for DF investigators to develop their skills to conduct DF investigations. One reason behind this is that in every country, there are different procedures and requirements for DF investigations. The levels of qualifications for acceptance of DF investigation reports vary among legal systems. For example, a country's law can influence the acceptance of DF practitioners or investigators according to their legislation.

All above mentioned factors are applicable to changes and upgrades, which certainly affect the process of digital investigations. The rapid changes in technology and excessive usage of the latest technology, highlights the need for continuous training and knowledge development to maintain the competency of DF experts. Therefore, when establishing DFC, the competency of the DF experts must be maintained because they are the show runners of the investigations.

2.4.3 Certifications in Digital Forensics

Despite the fact that DF is defined as a discipline, many academic institutions offer degrees in the field, and training remains an essential element in ensuring the competency and capability of the degree holders (Liu, 2016; Jones and Valli, 2011; Grafinkel 2010; Nelson et al. 2010; Furnell, 2004;). Therefore, many organisations offer training and certifications in DF. IACIS, ISFCE and High Technology Crime Investigation Association (HTCIA) are some of the main organisations which were designed to contribute and build common understanding in the field of DF (HTCIA, 2016).

IACIS provides a wide range of training throughout the year. The Certified Electronic Evidence Collection Specialist (CEECS) is the most basic examination for a certified course provided in IACIS. This CEECS certification means that the student has the ability of tracing emails, acquire evidence correctly, recover data, and other fundamental skills of a DF Investigator. The Certified Forensic Computer Examiner (CFCE) is considered the highest certification provided by the IACIS because it requires passing the tests. In addition, the CFCE requires recertification every 3 years in order to show continuous learning in the field of DF investigation (IACIS, 2016).

The High-Tech Crime Network (HTCN) offers a series of training courses in DF. In order to obtain one of the HTCN certificates, candidates must meet a number of requirements different from other organisations. HTCN reviews related training courses obtained by the candidate, sets written examinations and reviews candidates' work experience. HTCN offers Certified Computer Crime Investigator (CCCI) and Certified Computer Technician (CCT); all these certificates offered at the basic level and advance level certificates. All four different certificates offered in HTCN have some common requirements; however these requirements vary for each level. The advanced levels in both types of certifications require extra work experience in the required field, extra approved training in the same field, and the number of investigations involved should be at a higher level than for the basic level certificate (HTCN, 2016).

The ISFCE, which was established to professionalize DF, provides high forensic and ethical standards and conducts research in the development of DF. It also offers the Certified Computer Examiner (CCE) training which, interestingly, requires the candidate to provide a clean criminal record and pass three test modules, including a written and practical test (ISFCE, 2016).

There are a number of other organisations that offer certificates and a number of scholars encourage having widely recognised certification in the field of DF (Brill et al. 2006; Mayer et al. 2004; Taylor et al. 2007b).

2.4.4 Vendor Training courses and Certificates

Many of the common training courses in the field of DF are offered by the vendors or the software providers, where the vendors commit to supply the software and training. This includes the training of either a single buyer or a group of buyers (Guidance Software, 2016; AccessData, 2016).

This type of training has many benefits to the organisation because such training is usually peer reviewed by external bodies, well described and is normally supported with text books. In addition, they are organised to be available at different times in the year, which allows for as many personnel to participate as required. This process gives the opportunity

to examine the quality of the training and can be assessed by observing the experience of the participants who attended any other specific training course (Jones and Valli, 2011).

Guidance Software and AccessData are two of the world's leading private companies for supplying DF tools, and offer a wide range of training and certifications in DF. For example, Guidance Software, the supplier of the EnCase tool, offers certificates such as EnCase Certified Examiner (EnCE) and The EnCase Certified eDiscovery Practitioner (EnCEP). Such certificates are obtained after examinations and are valid for three years. The certificates are open for anyone holding a valid licence of the software (Guidance Software, 2016).

In the same perspective, AccessData, the owner of the FTK tool, also offers training in forensics, mobile forensics and also provides training related to legal issues. AccessData also provides certification of AccessData Certified Examiner, and AccessData Mobile Examiner and legal certification with a training leader (AccessData, 2016)

From the above, we can see that there are a number of organisations offering courses, training, and certification: private companies, non-profit organisations and universities. Certificates and degrees awarded by academic institutions require regular updating and, as a result, continuous learning is required to remain competent in the field. Courses offered by DF software tool providers are in demand by private and government organisations because they offer complete solution for their consumer's needs (Hewling,2013; Jones and Valli, 2011 Carlton, 2007;). Such organisations prefer to build a long term relationship with their consumers to make sure of continuous income and to assure the quality of their products.

2.4.5 Evaluating Training courses

In order to evaluate any training course we need answers to a number of questions that might be raised regarding the content, cost, and time of the training course. Examples of such questions are:

- Is the training worth the cost?

- Is the organisation getting value for the money from a specific training course?

Training courses and certifications in DF vary from one day courses to postgraduate university degrees which usually takes a couple of years to accomplish. Sabeil et al. (2011) conducted an extensive study into training courses in DF and argued that DF is not yet a mature field; as the training course providers deliver the training materials and are not very keen to provide quality education, which results in a poor quality of training on many occasions. In addition, some training providers are lacking in quality assurance assessment for the candidates and accreditation for their certificates from an official body.

To sum up, academic degrees offer basic coverage of the subject area, and courses offered without approved certification might not add value to the skills of the DF investigator. For such reasons, many organisations target certified courses and those offered by the software vendors to assure the competency of their trainees. Therefore a professional body to represent the training and certification in the field of DF might be helpful towards setting a minimum requirement for DF experts, training and certification and accordingly help in building DFC.

Summary

Training is a crucial factor in the field of DF development (Losavia et al. 2016), but sometimes it has a negative impact on organisations. DF training costs may be high and the outcome of the course might not improve the investigator's capabilities due to a number of reasons. In case where training result is successful and had a positive outcome, this might have a negative impact on the organisation because there is a chance that the qualified person either leaves the organisation for a higher salary job or pressures the current employer for promotion or extra allowance as the field of DF is sensitive and demanding**.** One way to overcome this issue is to train group of staff at the organisation such that missing one or two of them at a time will not hurt the organisation.

Education in the field of DF is another kind of training, especially in the computer science because there are no computer theories applicable which can be used and built upon. However, there are specific skills to learn in each case or scenario and certificates in this

field mostly last for a limited period and also require updating and continuous learning. It is in this sense that an organic and flexible but assured system of certification and education for DF is necessary.

2.5 Digital Forensics Tools and the selection process

In this section is discussed the DF tools, software and hardware, open source and commercial tools. Also this section provides the reader an understanding of how the DF tools selection process takes place in DF investigations.

DF tools play a vital role in the process of any DF investigation and therefore it is an important issue to consider the development of DFC. The functionality of tools has been developing and becoming more advanced in a very rapid manner. This section is organised as follows: section one will discuss the most commonly used DF tools; section two will study the ways organisations select and validate their tools; section three will measure the effectiveness of DF tools; and finally, section four will draw a conclusion by finding the effect of DF tools in the development of any DFC.

In the section below the current DF Tools available in the market will be analysed because research into DF tools is of interest to the academic world, especially with regard to determining the minimum standard for the reliability, admissibility, and functionality of a DF tool and how DF investigators help organisations in developing their DFC (Losavia et al. 2016; Harichandran et al. 2016). Hibshi et al. (2011) calls this the “usability” of DF tools. International Standards Organisation (ISO) ISO 9241-11 defines usability as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (Bevan, 2001).

2.5.1 Digital Forensic Tools Availability, Functionality, and Popularity

DF tools are widely available to support DF investigations. Brinson et al (2006) presented a cyber-forensics ontology model, provided an overview of DF and the stakeholders in the field, and offered examples of the tools that might be used on available platforms. DF Technology in Brinson’s model is divided into two subsections: software and hardware.

Additionally, Brinson's et al (2006), Volonino et al. (2006), Nelson et al. (2010), and Jones and Valli (2011)have agreed for the classification of tool that they are only of these types: open source tools, commercial tools, functionality-software tools and hardware tools.

This section discusses DF software tools and DF hardware tools, discussing the availability, functionality, and popularity of existing DF tools in both categories.

2.5.1.1 Digital Forensics Software Tools

A wide range of software tools are available for DF, such as EnCase, FTK, Sleuthkit, Raptor etc. (Wazid et al. 2013). As Encase and FTK are the most extensively used tools by DF investigators (Hasan et al. 2012), this section will discuss only two software tools, EnCase and FTK. A recent survey conducted by Hibshi et al. (2011), on the usability aspect of DF tools, showed that "out of 114 users, only 7 had never used FTK and only 6 had never used Encase" (Hibshi et al. 2011).

Hales et al. (2013) reasoned that EnCase and FTK are widely used by DF investigators for a number of reasons. Firstly and most importantly, both FTK and EnCase are accepted by the courts in many countries. Secondly, both tools are user friendly and they come with a Graphical User Interface (GUI). Finally, these tools provide a wide range of capabilities in the different stages of DF investigation and case management functions. Examples of these features are discussed below.

FTK and EnCase DF software supports different file systems such as FAT 12/16/32, NTFS, EXT2, 3 CD/DVD, HFS HFSX, and Solaris UFS. Moreover, they provide a number of searching capabilities such as Boolean, Hex, and regular expression searches. Further, FTK and EnCase have forensic analysis capabilities which allow the DF investigator to browse easily detailed sections of the image of the device under search. Finally, these tools have many reporting and exporting features which allow them to do XML, HTML and text reporting, and file and folder exporting of any investigation (Guidance Software, 2013; AccessData, 2013).

In the market, there are a number of other powerful open source DF tools which are used in DF investigations such as Sleuth kit and Autopsy. These tools have mostly the same functionality as the commercial tools. For example, they can perform analysis on live and imaged systems; also examine file systems without relying on the operating system, keyword searching, and image integrity. Finally, open source tools such as Autopsy provides case management with GUI (Manson et al. 2007).

The current trend of using DF tools within law enforcement departments is towards the use of commercial tools which are developed by private organisations. Commercial tools are usually delivered to the clients as a full package, and include software, training and maintenance. However, they are very expensive (Jones and Valli, 2011), despite the fact that EnCase and FTK are the most popular toolkits available. Sommer (2010) also states that the above mentioned tools are not tested to the standard expected for most forensic scientists. This shows that the popularity of a DF tool does not necessarily mean that it is error free but could be due to its advertisement.

“Daubert standard” is an extension of the Court’s earlier method to the acceptability of scientific evidence and results proved that many open source tools meet the standards to make evidence admissible (Carrier, 2002). For example, according to Mansion et. al (2007) where he compared Sleuth Kit to EnCase and FTK by running a number of tests on the three tools to find which gave the most correct results .This experiment concluded that each tool has strength and weakness, however he added that all three tools should be used in the academic environment including Sleuth Kit which is open source tool (Mansion et. al 2007). In addition, open source tools could be more effective and sometimes more practical than commercial tools, especially for organisations and laboratory with a limited budget for purchasing DF tools. Bukhari et al (2010) argue, however, that a number of open-source tools were originally designed for purposes other than forensics, and therefore they do not satisfy the forensics standards requirements.

While this debate remains to be resolved by the DF community, this author also believes that a DF software tool ought to meet the forensics standards requirements, and does so, at

minimum, when it meets the admissibility requirements in a court of law in those countries where the forensic investigations are being conducted or presented into evidence. This is often referred to by DF practitioners as the "court blessing" (Hibshi et al 2011). After all, the end result aimed at by DF investigation is to collect legally admissible DF evidence. As Hibshi et al (2011) stated: "These tools are typically used to conduct investigations of computer crimes by identifying evidence that can be used in a court of law." The admissibility of the DF evidence ought to be, thus, the primary factor for determining the choice for any DF tool. The other factor, according to Hibshi et al (2011), aside from "conviction support" is "investigative leads."

2.5.1.2 Digital Forensics Hardware Tools

The Digital Evidence (DE) is normally delicate as they may be taken in pockets of digital devices and can easily be damaged or destroyed. For example, opening a file might change the evidence because information regarding the date and time of accessing this particular file, which might be legally relevant and important data, might be modified. Therefore, familiarization with different investigative software and hardware tools is one of the essential awareness for the DF investigators when dealing with digital devices (Brinson et al. 2006).

There are a number of hardware tools available for DF investigators. These hardware tools have powerful features and allow DF investigators to deal with a range of existing devices. According to Nelson et al. (2010), hardware forensic tools can be divided into large, lightweight, and portable workstations conducting a number of functions according to their specifications and type of investigations.

The Forensic Recovery of Evidence Device (FRED) is one of the most widely used DF hardware tools by investigators, as it provides acquisition and analysis functions to investigators (Hasan et al. 2012). For example, the FRED system can acquire data from various types of hard drives, media devices, storage devices and many others with the feature of exporting the imaged data to another storage device. The FRED family includes

a number of DF hardware tools such as FRED-L, The UltraBay II, and Ultrakit III, which is a portable tool kit.

The DIBS Advanced Forensic Workstations and Digital Intelligence is another example of a complete DF hardware tool which also provides a range of acquisition and analysis functions. There are many other DF hardware tools such as the UltraBlock Forensics card reader, Image MASSter Solo, FastBloc, Acard and many others. Every DF tool has a specific feature and performs certain tasks. As such, tool selection in any investigation is subject to the incident scenario. For example, the ACARD SCSI-to IDE is widely used hardware tools in DF designed to conduct a single function, which is to assist the investigators as a write blocking device (Bidgoli, 2006).

Unlike the DF software tools, therefore, DF hardware tools are more reliable on the function of the hardware and the demands of the incident. Regardless, such DF hardware tools, like their software counterpart, ought to also meet the minimum standard requirement of admissibility in a court of law in those countries where the data are being collected and/or offered as evidence. The DF hardware tool must specially avoid putting the authenticity of Digital Evidence into doubt by modifying the data during retrieval, and safeguards against such intentional or unintentional modification of the target data during data acquisition and validation ought to be put in place.

2.5.2 Digital Forensic Functionality and Investigative Effectiveness

DF investigation goes through a number of different phases and, depending on the requirement, one or more tools are used in a particular investigation. This section discusses the tasks that can be achieved using DF tools, and the stages in the investigation in which these can be performed. After that the examples of the effectiveness of some DF investigative tools will be addressed.

Acquisition, validation, discrimination, extraction and reporting are the main tasks to be achieved using DF tools (Nelson et al. 2010). Making a copy of the original data available on any device is known as data acquisition, and this includes other sub-functions to ensure having an exact copy of the original data without any deficiencies. This is the first task that

is usually performed by DF investigators in any investigation. DF tools can be used “to make best-evidence duplicates and perform non-destructive analysis” (Hibshi et al. 2011).

Validation of copied data is also essential. This task can be achieved by using a number of tools and techniques to ensure the data integrity. DF tools also have data sorting to facilitate the separation of the relevant data.

Data extraction is considered to be the most challenging task because it involves data viewing, data searching, changing data formats, reconstructing parts of the data and finally bookmarking the data (Nelson et al. 2010). Currently, DF tools offer different styles for viewing data. This allows DF investigators to navigate and easily examine a device with a number of search options. Occasionally, DF investigators need to change the format of the data to be readable and some of the current tools offer the ability to change the format of the data, while other tools use third party software to do so.

DF investigation might not always be easy because an evidence file might have been deleted; therefore, this is an additional task to be performed. Recovering deleted items or data reconstruction is referred to as “salvaging” in Europe and “carving” in North America. According to Hibshi et al (2011), “contemporary analysis can recover deleted files, construct event timelines, attribute events to users, and much more.” Aside from deleted data, dealing with encrypted data is one of the major challenges in DF investigation, because files, disk partitions, drives and emails all can be encrypted and DF tools sometimes are not helpful in accessing such encrypted data. Finally, bookmarking is usually done to all data retrieved so it can be referred to when needed (Nelson et al. 2010).

DF tools also provide the option for the reconstruction of the suspect’s device. This gives the investigator the opportunity to understand how the crime or incident took place and the best results are produced when using the same make and model as the suspect’s device. Reporting is the final stage of the investigation process where the process of the investigation and the evidence is documented. DF practitioners have identified reporting as a difficult task, and suggest better reporting functionality for DF tools (Hibshi et al. 2011). Current DF tools, which are Windows based, provide reports in many formats such as

Word, HTML, and PDF, among others. In addition, they can also log and report every step the investigator undertook during the investigation (Nelson et al. 2010), a very helpful tool for reporting.

2.5.3 Digital Forensics Tool Selection

In any criminal or commercial case where digital devices are involved, the DF investigator should ask a number of questions about the effectiveness of the tool or tools to be used for that particular investigation. Before discussing the factors which help in selection of the appropriate tools for DF investigation, DF investigators must first confirm the legal admissibility of the DF evidence retrieved by a particular tool based on the tool's functionality and safeguards, so evidence does not become questionable in the court (Manson et al. 2007). Nelson et al. (2010) and Volonino et al. (2006) identified a number of factors about the DF tool selection, from which a DF investigator can make a decision on the most suitable tool to use for that particular DF investigation.

The type of device that is subject to investigation is one of the factors to be considered because evidence might be available on any media device. Windows, Mac, Android, and Linux release such as FreeBSD, Red Hat & Fedora are all examples of available operating systems. Despite the capability of some tools to deal with different file systems, at the same time the file system of the search device may affect the selection of tools. There are wide ranges of different file systems that exist today.

For example, most common file systems in use with the Linux world are: Fat16, Fat32, NTFS (For Windows Compatibility) and NTFS-3g are installed by default in Ubuntu, allowing Read/Write support, ext2, ext3, ext4, reiserFS, JFS, XFS. As Hibshi et al. (2011) observed modern DF tools must support a plethora of complex file systems, leading to specialised training courses and books on the subject. The status of the data is another factor which might force the investigator to follow a different approach, especially while dealing with live data unlike imaged data. Finally, the location of the data or incident may

also affect the tool selection for the DF investigation, particularly when dealing with imaged data, live data and data available in a Cloud environment.

Because the design of modern DF tools are what Garfinkel (2010) and Hibshi et al. (2011) calls “evidence-oriented,” it has created challenges for users such as “slow speed, inability to find non-ordinary information, lack of smart reporting functionality, and inability to construct a timeline that helps investigators in their analysis” (Hibshi et al. 2011). The evidence-oriented design of DF tools also requires that DF practitioners continually undergo training to keep pace with new technology (Hibshi et al. 2011).

Summary

Investigators in any DF investigation have specific missions and responsibilities to find any piece of data to form a case against a person or support the evidence. In this regard, investigation requires appropriate tools, and so DF tools are a crucial part in the development of DFC.

Current DF tools are very powerful and they can be used to reconstruct incidents, develop incident timelines, and log and report every action. In addition, DF tools have become more user-friendly and they are sign-posted throughout the process of the investigation. This might provide an environment for future DF investigators not to require an extensive knowledge in Information Technology to practice as a DF investigator. In the meantime, Reith et al. (2002) observed that existing DF tools are typically too technology specific and that they remain inconvenient for non-technical users. “Such users have typically been trained to use a particular tool, but may not have any foundational education about the underlying technology employed by the tool” (Hibshi et al. 2011).

There is a wide range of tools available for DF investigators to use. However, commercial DF tools seem to be used mostly among DF practitioners. The main reason for the wide use of commercial tools is because they are believed to be industrially approved, despite the fact that most of them have not been scientifically tested or approved. Regardless, evidence from both commercial and open source tools have been deemed admissible in courts, and

DF practitioners continue to rely on open source DF tools especially when the commercially available DF tools lack a function that is available in the open source tools (Hibshi et al. 2011).

Whether a tool is commercial or open source in nature ought not to be the most significant determinant for choosing a specific DF tool. Instead, depending on whether the subject of the DF investigation is software or hardware based, or both; the choice of a specific DF tool ought to be made from the point of view of (1) the legal standards for admissibility in those countries where the digital evidence will be offered as evidence, (2) the functionality of the tool, and (3) the needs of the incident, including the type of OS, the type of file system, the characteristic of the data such as the subject device, live data or cloud environment data (Harichandran et al. 2016; Bariki et al., 2011).

As to the third factor, perhaps DF tools will be designed in response to Garfinkel's (2010) criticisms of the drawback of "evidence-oriented" design for DF tools. One proposal for the DF tool is that it can performs automated analysis and reporting and that it can take into consideration systems, user interface, reporting intelligence, and user-friendliness to untrained investigators (Farrell, 2009). It is important that DF tools are user friendly to DF practitioners, as most DF practitioners are not programmers and are unable to write their own code (Hibshi et al. 2011). The study conducted by Hibshi et al. (2011) concludes that "current digital forensics tools are not considered user-friendly and that they lack intuitive interfaces."

2.6 Digital Forensics Legislation, Principles, Practices and Investigation methods

In this section the principles and practices in DF investigations are discussed. Legislations and jurisdictional issues play a major role in building DFC and when referring to the organisation structure and design theory to create a comprehensive environment there is need to focus on the most efficient way to group the tasks which will be discussed by using various examples.

The state of DF is now considered to be a scientific discipline also the National Research Council recognised DF as a discipline in the field of forensics (Losavia et al. 2016; Jones and Valli, 2011; National Research Council, 2009) because in many countries this field is governed by rules and regulations. In addition, the accuracy of the results, produced by the DF tools, allows it to be a professional discipline. Creating a standard for acceptable practices in DF also remains one of the essential challenges in the field (Harichandran et al. 2016; Casey, 2011; Nance et al. 2010; Garfinkel 2010; Casey, 2009).

This part provides a background of legislations, principles and practices available in the field of DF. In addition, it provides a background on DF investigation methods and an overview of DF development. It also concludes its effects on the DF stakeholders in developing standards and common practices in the field because developing guidelines and standards will provide a solid ground for development and future work in the field of DFC.

To date, the ACPO guidelines are regarded as the conclusive and best practice guide for computer forensics in the UK. ACPO covers police forces in England, Scotland, Wales and Northern Ireland. The "ACPO Guide" was created to provide guidance to law enforcement and those who assist law enforcement in investigation cyber security incidents and crime. It is constantly being revised in reaction to technological changes and the 5th version, published in 2012, moved from covering only computer based evidence to digital evidence that "encompass the diversity of the digital world" (ACPO Guide, 2012).

In addition to ACPO, particularly that relates to DFC, is the ACPO Managers Guide: Good Practice and Advice Guide for Managers of e-Crime Investigation the ACPO Managers Guide discusses the initial set up of a DF environment. The "Initial Set Up" section of the ACPO Managers Guide discusses the following concerns: role definition, training issues, budget, personnel, skill profile, line managers within specialist investigation Units, staffing levels, disciplinary issues within e-crime units, location and accommodation, internet auditing, accreditation, prioritization, health and welfare, security of data, and management information (ACPO Managers Guide, 2011).

Electronic Crime Scene Investigation (ECSI) which was published by the National Institute of Justice in the USA is examples of guidelines produced for first responders to deal with crimes involving digital devices (Ballou, 2010). In addition, recently, an Electronic Evidence Guide has been produced by the European council to add to the DF library for first respondents in crimes with digital evidence. Recently Montasari (2016) proposed a formal model to conduct digital forensics investigation. The production of guidelines to deal with crimes involving digital devices is a positive sign towards standardisation and future work.

DF is mainly keeping pace with the technology development of DF tools to deal with specific problems. The development in the field of DF with regard to investigation models also took place in the past years. However, there is no investigation model standing out as the standard in DF (Montasari, 2016; Casey, 2009). Efforts in DF are less focused to identify and agree upon definitions or standards for DFC, which is one of the goals of this research.

2.6.1 Digital Forensics Legislation

The use of technology is increasing among corporate organisations and also by individuals. Criminals take advantage of the power of digital devices and technology to commit crimes which are going on an increasing rate (Lillis et al. 2016; Nuth, 2008; Wang, 2007; Walden, 2004); therefore the involvement of technology in crimes demands finding and extracting evidence from digital devices a critical procedure. This is due to the sensitivity of the evidence that could be found to prosecute criminals which should be collected and presented in a way that is admissible in the court. Therefore the development of legislations globally should also keep pace with the increase in crimes.

DF has rapidly developed with regards to technology, providing powerful tools for evidence acquisition, searching and extraction, whereas legislations with regard to DF are still under development (Cole et al. 2015; Marion, 2010; Meyers and Rogers, 2004). There are number of reasons for the slow development of legislation in the field of DF. Geographical issues and cultural differences are common justifications for lacking an

effective law to prosecute cybercriminals (Marion 2010;Shapiro 1999). A good example of the delay in passing such legislation was given by Abdelbaqi (2016): the computer virus "I Love You" virus, which was created and released by a Philippine hacker who was caught but set free without any charges, because the country did not have a law to criminalise the act. However, one month after the spread of the "I Love You" virus, the Philippine congress passed the Electronic Commerce Law.

The Indian government introduced the Information Technology Act (ITA) in 2000 (Information Technology Act, 2000) regulating E-commerce and digital signatures, Later in 2008, the ITA was amended to bring greater clarification and definitions of crimes committed on the internet (Khan, 2016). The ITA still was not free from a number of difficulties. An example of the difficulties which were identified by Lallie (2012) in the ITA for digital investigation is that only the police officers with a certain rank (i.e. Superintendent of Police or SP) can handle the investigation. In other words any investigation handled by an officer ranked less than SP the investigation and procedure will be questioned and may not be admissible in the court and therefore one has to ensure the presence of an officer with a rank no less than superintendent in every police station at all times.

Similarly, The UK Computer Misuse Act of 1990 was criticized for not being updated and not defining new scenarios and examples of cyber-crimes (Coleman, 2003). The UK Computer Misuse ACT of 1990 was later amended, and the act now provides definitions of new scenarios relating to computer crimes and jurisdiction (Computer Misuse Act, 1999). For example, before the amendment, unauthorised access to a computer material was not considered a crime whereas after the amendment it became a crime which can be tried at the court. Also the offence of unauthorised modification of computer material has been replaced by the offence of unauthorised acts with intent to create damage by accessing the computer. Now, however, it is again time to amend the Computer Misuse ACT (Montasari et al. 2016; MacEwan, 2008) to bring it up to date with the currently employed technologies and crimes.

In the USA, Computer Fraud and Abuse Act (CFAA) was passed by Congress in 1986 as revision to existing computer fraud law .The Act has been amended a number of times in 1989, 1994, 1996, 2001, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act.

Schell and Martin (2004) stated in their report that there is "*an apparent lack of effective legislation against cybercrime*". While it has been agreed globally that the cybercrimes pose a significant problem, there is little consensus about how to pass laws to fight cybercrimes in the time effective manner (Cole et al. 2015; Goodman and Brenner 2002). As stated by Marion (2010) it is the role of countries to be proactive in legislating cybercrime and to regularly update their cybercrime legislation. Countries ought to be concerned to be proactive because they might be affected directly by cybercrimes and hence can pass rules to penalize such activities. So far, certain countries such as UK and USA are proactive in this regards and have successfully passed legislation to criminalise the misuse of technology, however many other countries are still struggling in developing or passing legislation with regard to the development of cybercrimes (Barclay, 2014).

Many international bodies have also fallen behind in creating a uniform set of cybercrime treaties. However, the Council of Europe's (CoE's) Cyber Crime Treaty of 2001 was the first and is currently the only global treaty on cybercrime, ratified by 23 countries and signed by 24 others without ratification, but ironically this treaty is not yet in force. The reason for not enforcing the CoE treaty might be due to lack of infrastructure and proper resources to trace and fight cybercrimes in certain European countries which have signed the treaty. Regardless the fact that the treaty is not in force, the goal of the CoE Treaty might have been to create a European standard and common policy for regulating cybercrimes.

The CoE Treaty defines cybercrimes and includes provisions governing cybercrimes related to terrorism, child sexual exploitation, organised crime, copyright infringement, hacking, and internet fraud. Furthermore, the CoE Treaty works as a framework for international

cooperation in the DF investigation process, prosecution, and extradition of cyber criminals (Furnell, 2002). While the CoE Treaty is an important step towards creating a global standard for regulating cybercrime, Marion (2010) criticizes it for being mostly a symbolic piece of legislation with "*a limited effect on cybercrime in the long-term*".

One reasons for the symbolic status of the CoE Treaty is that even signatory countries disagree by their policies and procedures for regulating and investigating cybercrimes. As argued by the critics of the CoE Treaty Convention, combating cybercrime is not a problem from the signatory countries, but the problem is from other countries which lack awareness of how to combat cybercrimes (Schell and Martin 2004). It is because of these different views, values and other major problems more attention is needed (Marion 2010; Sinrod and Reilly 2000). "I*n some cases, some countries may feel they do not have the jurisdiction over these offenses, thus leaving it to another agency to investigate allegations. Although some countries have established agencies to coordinate cybercrime investigations, others have not*."

According to Marion (2010), despite its symbolic legislative nature, the CoE Treaty serves multiple functions such as (1) public assurance, (2) moral education, (3) legislative model for other states, and (4) as a deterrent. Furthermore there is need for global action with the involvement of the United Nations. As stated by Marion (2010), "*because of the global aspect of the internet no single law in a single country*" will be effective in combating cybercrime. There is a dire need for international bodies to play a more active role in creating a standard for DF (Brenner and Schwerha 2004; Kellermann 2010; Marion 2010; Bryant, 2016),

2.6.2 DF Principles and Investigation methods

With regards to the DF investigation, there have been many models presented for the process of investigation (Agarwal et al 2011; Pollitt, 2007), but no single model has emerged as the standard for DF investigation (Casey, 2009). A good practice guide to conduct computer crime investigations has evolved in the UK and was presented by ACPO.

These DF guidelines have become widely accepted not only the UK but also the rest of the world.

DF investigations were initially identified as being carried out in four steps: acquisition, identification, evaluation and admission of evidence (Pollitt, 1995). Eventually, this practice became more complicated because of the addition of more steps and more devices to the process of DF investigation. At the first Digital Forensic Research Workshop (DFRWS) held in Utica, New York in 2001, a group of researchers presented a seven step process for DF investigation including identification, preservation, collection, examination, analysis, presentation and decision (DFRWS, 2001). Furthermore, Pollitt (2007) provided a historical overview of the development of the Digital Investigation process models by presenting 15 different models and arguing that DF "*is changing from craftsmanship into a true forensic science*". This statement became true because DF is a discipline that is tough in my institutions and profession (Liu, 2016).

Since the DFRWS workshop in 2001, which was held to create a model for DF investigation, many more models have been proposed. The workshop aimed to gather experts in the field of DF and establish a community to share knowledge in the field. One of the outcomes of this workshop was an agreement among the experts on the status of the DF at that time. Furthermore, the workshop outlined a number of different investigation processes such as identification, preservation, collection, examination, analysis, presentation and decision (Palmer, 2001). One of the crucial benefits of such workshops is that it sets up the basis and direction of the future research in the field of DF.

One of the initiatives for developing a standard DF investigation model was introduced by Reith et al. (2002), who studied different models for DF. His work is built on the classical strategy for Digital Evidence collection as conducted by police departments. The author argues that his model is an improved version of the one announced in the DFRWS as it was the basis for his model. In addition, Reith et al. (2002) encourages others to use his investigation model as an initiative and to provide a standard for the collection of DE.

The Integrated Digital Investigation Process model proposed by Carrier and Spafford in 2003 (Saleem, 2015; Shrivastava et al. 2012), which carries forward the earlier work and combines the physical investigation process along with the digital investigation process, is organised into five groups containing 17 stages. The End to End Digital Investigation adopted by Stephenson (2003) which contains 9 processes, merged the long digital forensic investigation process. This model was a target of improvement by Baryamureeba and Tushabe (2004) who recommended an amendment to Carrier and Spafford's (2003) Integrated Digital Investigation Model, and which became known as the Enhanced Digital Investigation Process. Baryamureeba and Tushabe (2004) added two phases to the Carrier and Spafford (2003) model (trace back and dynamite), and the reason for the addition was to separate the investigation of the digital device (primary crime scene) and the physical crime scene (secondary crime scene) to avoid inconsistencies.

The different models of cybercrime investigation focus on finding and presenting evidence in cybercrime investigations. For this reason, the cybercrime investigation model has been developed since cybercrimes existed. One example of such modes is Ciardhuáin (2004) model which provides an understanding of the process of cybercrime investigation, attempting specific steps such as presenting the information flow in an investigation rather than focusing on processing the evidence.

On the other hand a number of network forensic investigations frameworks also proposed by Erbacher et al. (2006) based on previous DF models for network forensics. Similarly, a framework to conduct cybercrime investigations was proposed by Freiling and Schwittay (2007) which included a combination of incident response and computer forensics. This combination aimed to enhance the overall investigation process by analysing digital evidence. Conversely, Perumal (2009) proposed a model that defines live and static data acquisition as the most important investigation process which eventually results in better prosecutions.

The Systematic Digital Forensic Investigation Model which was suggested by Agarwal et al. (2011) aimed in helping forensic stakeholders and experts to set up suitable procedures and policies in an organised way.

The Relational Reconstruction model was proposed by Ademu et al. (2011). This model addresses the necessity for reconstruction and interaction, emphasising the regular interaction of all investigation resources. In addition, Ademu et al. (2011) stresses the importance of the right experts using the right tools. The author also emphasizes the importance of distinguishing the victim's needs, from which better case results can be determined.

The DF investigation process and evidence acquisition was discussed by Haggerty and Taylor (2006), but this does not pay attention to developing and managing DF capacity. In addition, the prime focus of the study is on securing evidence, preserving the integrity of the original data, recording actions throughout the investigation, production of an audit trail and analysing the data collected. Efforts continue by scholars to improve cybercrime investigation models until recently Poonia et al. (2016) proposed a new investigation model arguing that till date there is no standard investigation model for cybercrime investigation.

The need for building a standard in the DF investigation process was encouraged by Pollitt (2007), because the examples presented earlier in this section focus on the process of the investigation and are not built on a standard model. Therefore, it is believed that in order to cope with the future challenges in the field of DF, standard models for the investigation process must be approved. However, from the investigation methods discussed above, we can identify four common patterns emerging in most examples (collection, preservation, analyses and presentation of data or evidence). As a result, this may be seen as a common outline for developing an investigation method in any DFC.

Summary

Here is provided an overview of issues related to DF legislations and practices and a historical overview of the development of the investigation methods with examples**.** This factor is also important in the development of DFC**.** Enforcing legislation is crucial for

developing DFC because the main reason behind digital evidence acquisition is to prosecute offenders. If the digital evidence is collected in an improper manner then it will be inadmissible in the court. From the above it may be seen that crimes that cause damage inside the society had great influence in the development and passing of legislation against the misuse of computers. In addition political influence may play a major role in enforcing such legislation to criminalise cybercriminals. Therefore it is believed that international bodies will play a key role in developing DFC.

2.7 Digital Forensics Challenges

This section presents the in depth study of challenges of DF and technical challenges including Cloud Forensics which could become an obstacle in the development of any DFC. Also certain Recommendations are provided to overcome those challenges.

In addition, this section identifies any organisational, social and professional influences on the development of DFC. The reason behind addressing DF challenges is the significant improvement in technology in our daily life. On the other hand, cybercrimes are also increasing, causing threats to many governments, private and commercial organisations (Karyda and Mitrou 2007). For example, cyber-attacks have been recognised by the UK National Security Strategy as a tier one threat (National Security Strategy UK, 2015).

This part is organised as follows: first it discusses the technical challenges related to DF and reviews challenges related to Cloud Forensics. Legal challenges with regard to DF are discussed in section 2 and section 3 summarises DF challenges.

2.7.1 Technological Challenges

Technological challenges arise in the field of DF alongside the massive expansion in the use of new media devices on new platforms and with different applications. The introduction of new technology is considered as a new platform for criminals to commit crimes, and a new set of challenges to society and law enforcement agencies (Al Fahdi et al. 2016; Dahbur, and Mohammad, 2011; Garfinkel, 2010). For example, DF investigators should be familiar with the latest tools and techniques which will enable them to deal with

crimes committed using new media devices. However, this is not only the challenge for the DF practitioners, but also a pressure for the other stakeholders of DF.

There are a number of technological issues which can be considered as a challenge to DF such as the huge size of data storage, the production of new operating systems, and the use of multiple devices, encryption, live forensics, new social media channels, and the monitoring of large streams of data across a network. These are all challenges that affect the future development of DF. Mobile phones are one form of technology in which new models and upgrading to existing models are produced regularly and considered as a challenge for DF because there are hundreds types of them are available in the market working on different platforms with high levels of capability and which makes it handy to be used by criminals. Furthermore, the capture and analysis of storage media is a time consuming challenge for DF investigators because personal computers are now fitted with terabytes of data storage which results in more required time of search and investigation (Al Fahdi et al. 2016; Garfinkel 2010).

Another problem identified by Garfinkel (2010) is that DF tools become obsolete quickly and this is not very useful because the release of new technologies make it difficult for vendors to keep their products up-to-date. It also makes the testing of the tools unrealistic.

To understand the implications of the DF challenges in the next sections, focuses on one example of the challenges mentioned above which is Cloud Forensics. In the next section, we will describe the nature of the cloud environment that has implication in the development of DFC.

2.7.1.1 Cloud Forensics

Cloud Computing provides cost effective services for enterprises and different solutions for users (Alqahtany et al. 2016; Ruan et al. 2011). For example it can save up to 37% of IT infrastructure cost by changing data centres to the cloud. Furthermore, the Cloud Computing business is estimated to grow and reach up to $270 billion in 2020 with a growth rate of 30% (Rani et al. 2016). Cloud Computing as defined by the NIST is “a model which provides a convenient way of on demand network access to a shared pool of

configurable computing resources (e.g., networks, servers, storage, applications and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Islam Rahaman, 2016; Mell and Grance, 2010).

Cloud Computing provides different models of services depending on the environment of the service model used by the provider. For example, the Software as a Service (SaaS) option allows customers to use the provider's software, such as Google calendar and Google drive. In addition to the SaaS there is a Platform as a Service (PaaS) which runs on a cloud infrastructure but with limited permissions on the application level and no control over the network or the servers (Islam Rahaman, 2016; Zawoad and Hasan, 2013). Whereas the Infrastructure as a Service (IaaS) model is where the customers are given their own space and allowed to launch their own virtual machine with complete control on the storage, operating system and application and limited control of selecting network components. The IaaS is more adaptable for companies because they do not need to make changes to their applications in order to migrate to cloud computing (Herbst et al. 2015; Khajeh-Hosseini et al. 2010).

Cloud service can be "categorised depending on the deployment model private cloud, public cloud, community cloud and hybrid cloud" (Mell and Grance, 2010). Cloud is a multiuser environment for space which makes it cost effective where cost of service is counted per usage of service. In the same perspective, these advantages create challenges for DF. In the next section, we will study the reason for cloud being a challenge to the development of DF.

2.7.1.2 Why cloud is a challenge to DF?

Cloud Forensics is the application of DF principles and procedures in the Cloud environment. This is considered to be one of the significant challenges currently facing DF because Cloud Computing is growing very fast and attracting a large number of consumers and service providers. Cloud Computing provides a number of solutions in a cost effective way (Alqahtany et al. 2016; Ruan et al. 2011). The advantages and flexible features of

Cloud Computing create challenges in the development of the DF. The next section will present examples of these challenges.

Firstly, according to the features and deployments models described earlier, in the cloud environment there is no local storage data stored on a remote system where multiple users use the same storage. This situation causes an implication for DF investigators trying to access suspect files because there might not be a physical storage where the investigator can access the suspect's files. Thus, it may be difficult to avoid violating the privacy of other people's files and to clearly identify the crime scene (Masood et al. 2016; Guo et al. 2012; Wolthusen, 2009).

Secondly, the absences of physical storage of evidence of crime creates problem especially when seizing the personal computer of the suspect, because it is important to access files which will not exist on the PC, but stored in the cloud (Masood et al. 2016; Guo et al. 2012; Birk and Wegener, 2011; Dykstra and Sherman, 2011; Reilly et al. 2011; Wolthusen, 2009).

Thirdly, in cases where a DF investigator finds the required files of the suspect in the cloud environment, it is difficult to identify the suspect's data from other users' data (Birk, 2011).

Finally, counting on the cloud service provider for information about the users of the service and data owners are additional challenge. This problem identifies that the only party that holds the details of the customers is the provider of the service. In other words, the cloud service provider's statement may be the only evidence to link the data to a suspect (Masood et al. 2016; Guo et al. 2012; Dykstra and Sherman, 2011).

To sum up, Cloud Computing provides great solutions for users and organisations in a very cost effective manner. However, it also brings a challenge for the development of DFC. Recent research in DF has proposed solutions to overcome the challenges of Cloud Forensics which will be presented in the next section.

2.7.1.3 Proposed Solutions

This section will discuss a number of solutions suggested by researchers to overcome the challenges of Cloud Forensics. Digital signature is proposed as one of the solutions for the integrity of distributed data. Hegarty et al. (2009) proposed a framework to detect distributed signatures because of the nature of the Cloud environment; and according to Zawoad and Hasan, (2013) this framework has made a positive contribution which will aid help DF investigators. The cloud environment is complex with multiple consumers sharing a space option which becomes a problem when seizing information. Therefore, Delport et al. (2011) suggested isolating the cloud instance to avoid the exposure of evidence to corruption and loss of data. A cloud management plan is one of the suggested solutions for the dependency on the cloud service provider as being the only party to provide information for data acquisition (Dykstra and Sherman, 2011).

Cloud computing is growing with greater challenges arising and solutions being suggested. From the above examples, we believe that the consumer is helping to put more pressure in the development of DF by shifting to new technology. New technology is putting more pressure on DF investigators in terms of dealing with them although there are initiatives from scholars in the field to overcome such challenges. Governments and other international bodies have not made any serious attempts to address the issues except through the educational institutions and manufactures in conferences and workshops.

2.7.2 Legal Issues and challenges caused to DF development

Cybercrimes are increasing, taking different shapes, and are being committed across borders; these are important issues that need to be addressed (Nance and Ryan, 2011). The internet provided a platform for both vendors to offer their services and for criminals to commit crimes. Both are operating across borders, which raises a number of issues such as jurisdiction, privacy and intellectual property, contractual issues between vendors and consumers and many others (Nance and Ryan, 2011). The technological advancement creates a legal issue which eventually become a challenge for the development of DF.

In fact, the most important part in the whole process of DF investigation is the admissibility of the collected evidence in court proceeding. The admissibility of the digital evidence is crucial because the law has very strict rules in order to accept a piece of evidence into the record of a court proceeding. To be admissible, evidence has to be shown to follow the chain of custody, and that the evidence is authentic. The chain of evidence requires showing that the evidence has not been tampered with or corrupted. The requirement of authenticity requires the showing that the evidence is what the proponent claims it to be.

For example, the Cloud environment provides extraordinary features to its users, one of which is allowing a multi-tenancy occupation of a certain space. This raises another challenge for the DF investigator because the investigation process always requires a clearly defined crime scene which is not always guaranteed in such a cloud environment. An undefined crime scene or a multi-tenancy occupation makes it difficult to attribute the data to the suspect, and additional proof has to be provided for such attribution. The multi tenancy occupation adds another layer for the DF investigators to uncover. In addition, the privacy of other tenants' information is possibly vulnerable in the process of uncovering such a layer (Masood et al. 2016; Zawoad and Hasan, 2013).

The remote access to data storage and applications also creates added challenges to proving jurisdiction, to conducting an investigation, and to proving the identity of the suspect. Cloud computing allows countless users to store data in one location, wherever the service provider places the storage system, and it also allows a user to store data remotely in multiple remote locations at one time. The mass remote storage of information creates issues of technological capacity to review such mass storage, and at the same time, the multi-site remote access multiplies the problem and adds a layer of jurisdictional issues, especially since not every countries have laws in place that are DF investigation friendly.

Criminals attempt to plant obstacles for DF investigators by developing methods and techniques; this is referred as anti-forensics. The goal of these techniques is to avoid the discovery of events, cause disruption for the process of data collection, increase the time of investigation and create doubt with regard to the evidence. These techniques raised in the

field of DF may be in the forms of data wiping, data hiding, encryption and data corruption (Dahbur and Mohammad, 2011).

Summary

From the above it can be summed up that the technological advancements are a great aid and at the same time there may be legal challenges. As a result, they become a challenge to the development of DF. The world is witnessing a fast growing computer capability as a response to the needs of business, but the world is not developing rules and regulation to cope with the implications that can be caused by these developments. Therefore, the researcher data in the next section explains the importance of organisation theory and how they can contribute to the development of DFC and overcome the challenges faced.

2.7.3 Organisation Theory in Digital Forensics

This section elucidates the role of organisational theory in DF. Firstly, this author explains what organisational theory is, including its definition, the competing theories in organisational theory, and the different perspectives in organisational theory. Secondly, this author offers a definition for DFO by explaining DF and the DFOs. The section offers a definition for DFO. Thirdly, this author explains the role of organisational theory in DF, and how organisational theory could generate DFOs, and therefore DF investigation is more efficient and capable. Finally, the author argues that DFOs must create a framework for establishing and managing a DFO using an organisational theory concept.

2.7.3.1 What is Organisational Theory

Organisational theories can act as professional and scientifically approved methods to solve an organisation's complicated problems and help them organisations to move from their current state to a desired state (Cunliffe and Luhman, 2012). However, explaining the concept of organisational theory is not an easy task. The importance of organisational theory, however, cannot be overlooked. It is difficult to understand what people do and how they do it, and why they do it, without looking at the organisations in which people function. Organisations are defined as social units of people that are structured and managed to meet a need or to pursue collective goals. In this sense, organisations are social

units that require structure and management, a definition that applies today to almost all human endeavour. However, according to Parsons and Jones (1960, p.17), “primacy of orientation to the attainment of a specific goal or purpose is used as the defining characteristic of an organisation which distinguishes it from other types of social system.” Schein (1970, p.9) describes an organisation as “the rational coordination of the activities of a number of people for the achievement of some common explicit purpose or goal, through division of labour or function, and through a hierarchy of authority and responsibility.”

In order to explain organisational theory, one needs to describe the concept of theory, which is not easy to define. The define if a theory is a set of statements or principles, devised to explain a group of facts or phenomena, especially one that has been repeatedly tested or is widely accepted and can be used to make predictions about natural phenomena. Theories matter because they influence what happens to people; they are used to describe, explain and, equally significantly justify the things that we do and how we do them (McAuley et al. 2007).

Based on the above explanation of what an organisation is and what a theory is, one could state that organisational theory is about “conceptualizing, explaining and ultimately guiding action regarding the different ways in which people act in unison together to achieve particular, desirable shared ends or ‘common’ organisational goals” (McAuley et al. 2007). In other words, organisational theory is the sociological study of formal social organisations, such as businesses and bureaucracies, and their interrelationship with the environment in which they operate.

According to McAuley et al. (2007) “it is important that organisational theory should aim to improve organisational efficacy and efficiency in relation to those goals. That is, organisational theory can and should contribute to enabling organisations to successfully achieve those goals (efficacy) with as little use of its resources as currently feasible (efficiency).”

Over time, organisational theory has developed into three types: bureaucracy, rational, and division of labour (Lægaard and Bindslev, 2006). While it is beyond the scope of this thesis to go into detail as to each theory, each theory provides advantages and disadvantages to an organisation. Further, it is worth noting that many theories about organisations have evolved through the years, from the classical, to modernist, neo-modernist, post-modernist, and reflective theories about organisations (Lægaard and Bindslev, 2006).

2.7.3.2 What is a DFO

A DFO, based on the above description of organisations, may be defined as a social unit of people engaged in DF that is structured and managed to meet the needs or to pursue collective goals that are related to DF. Primarily, DFOs are a group of people in the field of DF with the collective goal of achieving a successful DF investigation.

There are, however, groups of people in the field of DF that may not necessarily be directly involved in DF investigation, but become part of the DFOs. For example, in the public sector, there may be officers in law enforcement who oversee the DF investigators and are not involve in the investigation process and the same with the public prosecutors who investigate.

2.7.3.3 The role of organisational theory in DFOs

Organisational theory can play a significant role in improving the efficacy and efficiency of DFOs. Since it is important that organisational theory improves the efficiency and efficacy of any organisation, the same is also true concerning DF. At present, however, there has not been a thorough study as to how organisational theory may improve DFOs.

This research proposes a theoretical framework that provides a definition on how a DFO operates by looking at three aspects that are studied and measured by organisational theory: infrastructure, human resources, and organisational policies. Organisation structure and design theory which according to Cunliffe and Luhman (2012) "focuses on the most

efficient way to group tasks, resources and people to achieve organisation goals furthermore it focuses on optimising the performance of the organisation to the demands of the competitive environment" . This could be applicable to a number of key factors in the proposed research, particularly the factors related to human resources such as training, education and certification.

It is necessary for DFOs to create and operate within a framework in their establishment and management. Because failure to do so will expose the DFOs and make DF investigation vulnerable to gaps and security breaches that could lead to future legal challenges. For example, a DFO that lacks the necessary organisational policies regarding the use of smart phones or external hard drives within DF laboratories may find itself in a situation where the DF investigator's neutrality may be challenged in court regarding privacy issues. Therefore, the Flexibility Theory could be the solution for an environment which faces the challenge of the rise of new technology and gives the option to the organisation to adopt the change (Cunliffe and Luhman, 2012).

By looking at these three factors, one could implement a framework for determining whether a DFO has achieved minimum efficiency. The author defines a DFO that has achieved minimum efficiency under organisational theory as a DF Capable organisation.

2.7.3.4 Organisation Theory in this Research

In this research is presented that the organisation theory is applicable in three perspectives. This research also focuses on the infrastructure of the DFOs to identify the patterns, look at the organisations, and the relationship of the divisions within the entity with each other. It also focuses on the HR of DFOs, which further focuses on the relationship of the members of the DFO with each other. Finally, this research focuses on the organisational polices which current DFOs have to organise and manage the relationship of the DFO with other organisations in the community.

2.7.4 Summary and Conclusion

Many of the above factors that have been reviewed are considered important to understand the development of DFC. The findings reveal that the infrastructural issues are one of the key concepts in the development of DFC. Secondly, DF training and certification are important factors, because without proper training and expertise in DF investigation techniques, investigators might face difficulty in handling investigations. Thirdly, DF tools and their selection play a major role in the collection, preservation, analysis and reporting phases. Finally, DF principles and practices are important as these ensure the integrity of the evidence collected from digital devices. This study has conducted an empirical research on all the above mentioned topics to develop DFC framework.

It is important to measure the effectiveness of the current guidelines in DF by conducting extensive data collection from a number of organisations. It is also important for organisations to prepare and implement security policies to be ready to handle digital evidence in case of criminal activity. The next chapters will show how the work was undertaken to find out the challenges faced by organisations in developing DFC and to suggest a framework to conquer those challenges. This was achieved by conducting site visits of organisations in order to understand the requirements for building and implementing DFC with proper staffing, training, selecting tools, management and governance and also to examine the challenges faced by such organisations to develop their forensics capabilities.

In Conclusion, the literature review provided an overview of the existing work done in DF, identified DF training needs, discussed most commonly used DF tools and how organisations select these tools, DF development, research, infrastructure and organisational, social and professional influences on the development of DFC. The next chapter will describe the methodology for data collection which will be followed for this research.

Chapter Three: Research Methodology:

3.1 Introduction

In this chapter is defined the research methodology implemented in this research, to investigate the stages and procedures followed by organisations in developing their DFC. First of all, the chapter shows how important are the research questions and how they were formulated and reviewed. Then, introduces three research principle models: the positivist, interpretive, and critical paradigms. Then, it clarifies the research strategies, data collection and data analysis methods. Previously, chapter 2 provided specific background literature in the research area by answering a number of the research questions. Throughout this chapter, the author attempts to provide justification of all the strategies chosen for this research i.e. research philosophy, research strategy and research method by providing a detailed explanation of each. This chapter then explains the research design for integrating interviews with grounded theory. Finally, it provides the criteria used to evaluate the quality of the research.

3.1.1 The Importance of Research Questions and Research Objectives

Research questions are essentially required normally enforce the researchers to explore and investigate in certain areas of knowledge. They are one of the key elements of a research project because they provide a number of guidelines throughout the research activities.

Research questions can be in the form of a statement that identifies the phenomenon to be studied (Campbell et. al., 1982). They normally contain a number of fundamental questions such as research purpose, objectives, data collection and conclusion. An essential part of the research is to have clearly defined questions and used at the initial stages of the research. As, according to O'Leary (2009), they "Define an investigation, set boundaries, provide a direction and finally act as a frame of reference for assessing your work" .Therefore research questions are crucial.

Research questions usually starts up with an investigation from which one can identify a topic, outline interesting questions, and describe the constructs and variables, the relationship between these issues and describe how research will end (O'Leary, 2009).

Wilson and O'Leary (2010, 2009) agree that good research questions set boundaries for a research project. In fact, research questions provide throughout the researcher a path because they help in determining the theories that are needed to be explored, the literature to be studied, the data to be collected and analysed. In addition, research questions also evaluate and measure the performance and quality of the research by comparing the research outcomes and determine whether they provide correct answers to the questions (O'Leary, 2009).

After determining the importance of research questions it is also vital to know how best to formulate the questions in order to achieve the most benefits and make the best decision. Therefore, in the next section we will demonstrate example of the process of generating research question.

3.1.2 Formulating Research Questions

In this section, the researcher presents methodology for generating research questions as suggested by O'Leary (2009).The methodology consists of four steps and each step consists of a number of questions which help the researcher to know what are required and what direction one could take (O'Leary, 2004).

Then the researcher applies O'Leary's methodology (as presented below) into this research and explains how the researcher formulated and presented the questions and objectives. These methodologies for generating questions allows reviewing of literature prior to identifying any gaps in the literature and use them as a guide for generating original question for research. This approach of examining the literature, prior to or while formulating the questions, is appropriate because Straussian Grounded Theory methodology, as applied in this research, also allows for a reviewing of pre-existing literature prior to conducting the research. In short, O'Leary's method for generating questions is consistent with the research methodology employed throughout this research.

Below are presented the four steps suggested by O'Leary (2009) suggested four steps in order to formulate the research questions:

Step One: consists of a number of questions, which should be answered in few words. For example:

- What is the topic?
- What is the context of the research?

Step Two: aims to find out the goal of this research and should consist of question that defines the target of the research, For example:

- What is the aim of this research?

Step Three: at this stage the researcher should ask questions to find out the nature of the research, For example:

- What is the nature of the research questions?

Step Four: finally the researcher to ask questions to find out if any relationships that could be established or discovered in the data, for example:

- Are there any potential relationships you want to explore?

In this project the researcher applied the four steps suggested by O'Leary (2009), and formulated the research questions. In step one the researcher identified the topic and context of this research by asking questions that could provide answers in few simple sentences such as Building and managing DF. In step two the researcher aimed to identify, document, and analyse the attitudes and practices of organisations in creating a DFC. In step three the researcher formulated the questions by exploring 'what is the DF system and organisation, who are involved in it and what are the protocols and tools used in the system of the organisation. In step four the researcher asked questions to find out how the organisation is put together, how the staff and personnel get trained, and why it is important to analyse the setting up, creation, and management of a DFO.

3.1.3 Formulating a Good Question

In formulating good research question, O'Leary suggested a five step process in a checklist to determine whether the research question(s) are applicable at practical levels as follows: (1) Is the question right for me?, (2) Is the question right for the field?, (3) Is the question well-articulated?, (4) Is the question doable?, and (5) Does the question get the tick of approval from those in the know? And the answers are:

First, the questions above are right for this research because they would help in developing DF field. They could be applicable to any organisations.

Second, the questions are right for the field because they extend existing scholarly work by asking whether the standards for creating and managing a digital forensic system are universal and standardized, and if so whether they are sufficient and effective when applied to other organisations such as Law Enforcement in Dubai. This research, which is based on the methodologies identified in chapter 3, will add to this scholarly work by looking at the applicability of their proposals to organisations that are building their DFC from the ground, and which have different legal, social, and cultural challenges.

Third, the question is well articulated for the research to progress successfully, and the researcher expects to continue to improve the questions as the research progresses.

Fourth, the questions are achievable because the researcher has access to the existing scholarly works on the proposed researched topic, and enough contacts in the field of DF.

Finally, current literature supports this research i.e. marked by references regarding the research objectives and research questions.

3.1.4 Review on the Research Questions

The research questions are divided into four main areas of DFC. In chapter 2, the author attempted to answer the research questions and these were partly answered. Therefore, the following section covers the unanswered questions that the researcher will answer in further chapters by using the method/methodology chosen in this chapter.

Question one is about the recommendations available in the literature in building a DFC; this was discussed in chapter 2. However, the literature fails to provide an answer on how effective and how widely such recommendations are followed and used. Therefore, this question is considered to be answered to some extent and will be researched and answered in more detail in the next chapters.

Question two in this research was also discussed in chapter 2 and proved that there is no standard methodological framework for setting organisational policies or addressing ethical and privacy issues. In chapter 2 the role and the activities of the international and national bodies in developing a standards for DF was discussed.

Question three focused on the managerial framework for DFC. The literature discussed in detail the issues related to Human Resources (HR) such as qualification, certification and training. Chapter 2 identified DF training needs and how the Digital Evidence (DE) is influenced by training and certifications. Chapter 2 also identified that DF does not have any recognised body for professional representation that requires even minimal professional educational standards to become a DF professional, therefore this question is considered as partially answered and requires further investigation and research in order to fully answer the question.

Question four discussed most commonly used DF tools and how organisations select these tools and measure the effectiveness of the DF tools. Chapter 2 provided a list of the available tools used in the field of DF, in addition, it discussed issues related to the credibility and approval of such tools but did not provide details on how effective DF tools are. In this regard, this research will investigate and research the remaining unanswered

research questions using appropriate methods. For further clarification and confirmation to show the direction of the research, below are the unanswered questions:

1. How widely recommendations in DFC building are used.
2. Is there a standard pattern identifiable in developing DFC between private organisation and government?
3. How do personnel in forensic professions recognise and manage pressure from various stakeholders on their professional practice?
4. How are training needs met i.e. what measures (technically/qualification wise) do organisations take while training their employees in DF?
5. What are the tools that are most frequently used in DF investigation? In addition, How/Why do they choose a particular tool? i.e. do they choose based on the effectiveness for a particular type of case etc.?
6. How can the present proposed research into DFC improve tools selection process?

3.1.5 Literature Research Characteristics

Research methodology is a scientifically approved approach to collect, interpret and analyse a set of data. O'Leary (2009) stated that methodology *"Provide both the strategies and grounding for the conduct of a study"*. There are number of factors that need to be considered before choosing any methodology for research i.e. Research Questions, Ethics, Time, Money and Territory, therefore next section will describe the characteristics of this research and, based on that, the choice of the research approach will be provided.

Research methodologies are designed according to the aims, purpose and data will be collected in relation to the stakeholders of the research as Flick (2015) suggested that in order to make a decision on your methodology it is crucial to look at the characteristics of the data that the researcher will deal with. This research aims are to identify, document and evaluate the stages and the procedures followed by organisations developing their DFC and to propose a framework which can be used to develop DFC. In essence, this research aims to discover and propose a theory or hypothesis for them.

In addition, this research is the type that investigates to understand the underlying procedures in developing DFC. This research provides insight of how to develop DFC and uncover prevalent opinion or thought in building DFC.

On the data collection side, the stakeholders of this discipline are well known, such as Law Enforcement Agencies, Private DF Investigators and academia. Finally, these research outcomes provide an explanation on how they have developed their DFC and then these research results can be made useful as a guide for organisations to develop their DFC.

3.1.6 Overview of Research Methodologies

Pickard (2007) classified research methodology in a hierarchal structure; this hierarchy provides levels of views to the research methodology. For example, the highest level expresses the philosophy of the research or Research Paradigm, which helps identify/choose a model or pattern that this research is based on, for example Positivism, Interpretive and Critical, which is considered most common in Information Systems (Jones and Karsten, 2009; Orlikowski and Baroudi, 1991; Chua, 1986**).**

The second level in Pickard's hierarchy for research is the methodology such as Qualitative and Quantitative methodologies. A qualitative methodology is data collection and analysis techniques that researchers use to provide descriptions to build and test theory. Qualitative research can also be a number of methods to focus on in-depth understanding of human behaviour in experiences and perceptions in order to understand decisions made. On the other hand Quantitative methodology is a technique which the researchers use to predict and control problems by measuring, evaluating and replication. It uses numerical data and measurable variables and the data are collected under controlled environment. These types of research methodologies are represented in different forms. For example Case Study, Grounded Theory, Narrative Study, Ethnography and Phenomenology which will be discussed in a more detailed in the next section.

The figure below shows the hierarchy of research methodology according to Pickard's classification providing examples for each level. After that will be provided an explanation of each level with examples in sections 3.2: Research models, 3.3: Research Strategy and 3.5: Data Collection Methods.

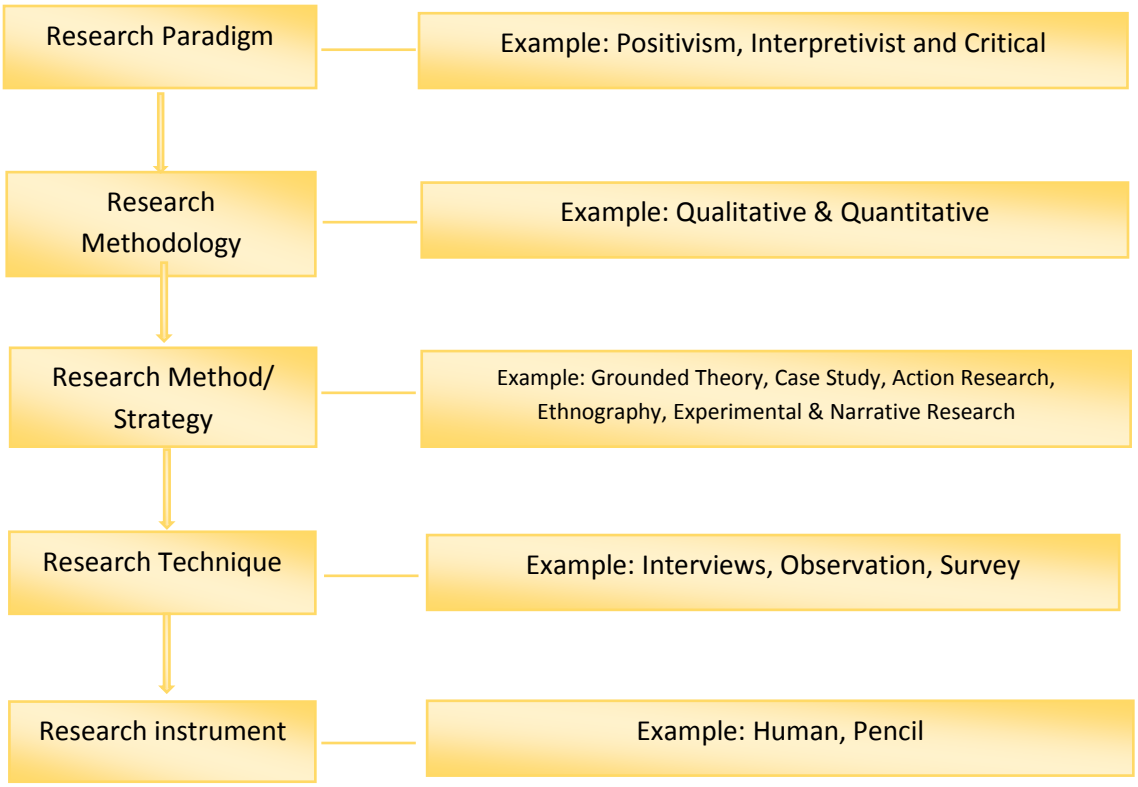


Figure 1 Research Methodology Hierarchy

3.2 Research Models / Paradigm

Research Models or Paradigms vary and each described concepts in the real world according to the way they gather information. Orlikowski and Baroudi (1991) stated that the researcher should base the research interest, direction and assumptions on an appropriate research paradigm. Therefore, it is important to choose the appropriate paradigm to address the main research questions, the most common of which are positivist, interpretive and critical paradigms (Orlikowski and Baroudi, 1991).

3.2.1 Positivist

Positivism or Logical Positivism, which is part of the scientific method, has been the leading research paradigm in the past several centuries (O'Brien, 1998; Oates, 2006). The aim of positivists is ultimately to state generalized rules or laws that come from mathematically determined statistical relationships of variables, derived from quantitative measures (Oates, 2006). Positivists research, according to Neuman (2011, p. 95), uses "precise empirical observations" in order "to discover and confirm a set of probabilistic causal laws that can be used to predict general patterns of human activity." In other words, positivism views phenomena as being subject to natural laws that a researcher can discover through logic and empirical testing using inductive and deductive reasoning. Therefore, positivists believe in an objective reality that independent observers can directly experience and verify. Positivists have used surveys and field experiments in their methodology (Choudrie and Dwivedi, 2005).

There are advantages and disadvantages to positivism as a paradigm. The advantages are to minimise bias and increase reliability through wider sampling (Chen and Hirschheim, 2004; Gable, 1994), while the disadvantages are that it treats people as mere numbers while ignoring historical, cultural, social, political, and contextual environments (Neuman, 2006; Collis and Hussy, 2003; Orlikowski and Baroudi, 1991).

3.2.2 Interpretive

As a reaction to the limitations and disadvantages imposed by the positivist research paradigm, the interpretive research paradigm emerged over the past half century, placing emphasis, unlike positivism, on the relationship between socially, culturally, politically, economically, and contextually influenced concepts and language.

According to Neuman (2011, p.102), the interpretive paradigm involves "direct detailed observation of people in a natural setting in order to arrive at understanding and interpretation of how people create and maintain their social world." In this regard, the researcher must maintain objectivity, acting as a passive collector and interpreter of subjective data (O'Brien, 1998). The interpretive paradigm views knowledge and reality as

social and language constructs, and therefore views “the social meaning of [a subjective] reality as explained by an individual or group” to be influenced by culture and history (Guo and Sheffield, 2008). In other words, interpretive paradigm researchers believe that they can better understand the social world within the context of the human environment rather than through quantitative and mathematical means (Bryman, 2008; Saunders et al., 2003).

Interpretive researchers have used methodologies such as case study, phenomenology, ethnography, hermeneutics, grounded theory, and participant observation (Choudrie and Dwivedi, 2005). The disadvantages of the interpretive paradigm that have been subject to criticism seem to be the opposite of positivism and include the generalisations of interpretive paradigm due to its lack of a wide sampling of a population and also that interpretive paradigm may ignore historical changes over time (Orlikowski and Baroudi, 1991).

3.2.3 Critical

The most recent addition to the research paradigm involving information technology is the critical paradigm, which has become a third alternative to the more conventional positivist and interpretive paradigms (McEvoy and Richards, 2006). Critical paradigm, is evaluative, critical, and aims to change the social reality of the research subject, is often associated with action research strategy (Choudrie and Dwivedi, 2005; Orlikowski and Baroudi, 1991).

Unlike positivist and interpretive paradigms, the critical paradigm research does not end at passive observation, understanding, or interpretation, but also aims to criticise and change relationships, conflicts, and contradictions that the researcher deems restrictive and alienating (Oates, 2006; Myers, 1997).

3.2.4 Model selection for this research

The interpretive paradigm is most appropriate as applied to DF and organisational theory because DFC deals mostly with a system composed of people’s interactions with information or data, which are social in nature. Qualitative research like that of the

interpretive paradigm focuses on social interactions and is therefore most applicable to information technology, specifically DFC (Fernandez, 2004).

The positivist paradigm would not be the most appropriate in a research that aims to propose a framework for the DFC of an organisation because this research studies organisations and people's behaviour. In addition, it studies people's interaction with the infrastructure and policies (or language) of a DFO and does not require figures in order to prove facts. The positivist paradigm could be helpful in enhancing the research with a survey to strengthen the research's position on the needs of a DF system and framework. The positivist paradigm, however, would fail to consider the historical, cultural, social, political, and contextual environments of a DF organisation.

The critical paradigm would not also be appropriate, as the research, here into DFC, does not aim to change the current DF practices and organisations, but to create a framework that would improve DFC. The critical research paradigm, however, may be used in some points to criticise weaknesses and vulnerabilities of DFC.

3.3 Research Strategy

The research strategy is, researcher's approach to answer the specific research questions posed (Saunders et al. 2003, p.9; Robson, 2002). There are various research strategies employed by researchers in the field of DF. The research strategies, discussed more fully below, include (1) Grounded Theory, (2) case study, (3) action research, (4) ethnography, (5) experimental, and (6) narrative research. After explaining each option for the research strategy, the author provides reasons for adopting Grounded Theory as the most appropriate research strategy for the research.

3.3.1 Grounded Theory

According to Glaser & Strauss (1967), a researcher may use Grounded Theory to generate or discover a theory based on an analysis of data. Martin and Turner (1986) defined the methodology as "an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously

grounding the account in empirical observations or data." In the end, the researcher can use the discovery of the theory from data systematically obtained from social research to explore integral social relationships and the behaviour of groups.

Grounded theory requires the collection of data in the field rather than through literature review. As such, the primary data collection methods include interviews, observation and document analysis. The researcher then deals with the data in two stages: (1) the selection of data, which involves theoretical sampling of data based on the potential contribution to development theory; and (2) data analysis and coding into categories. The second process involves:

1. Identifying categories in data
2. Building relationship between categories
3. Grouping categories together to form a theoretical construct

One disadvantage of Grounded theory is that the amount of data collected is usually large and may be difficult to manage and analyse because there is no standard rule to deal with Grounded theory data. Additionally, there can be difficulty in predicting the sample to be used (Denscombe, 2007).

3.3.2 Case Study

This method brings an understanding of a complex issue or object or it adds strength to what is already known through previous research. Another explanation of case study could be an exploratory analysis of a single person, group or event to find underlying principles. The primary data collection for this method is through interviews, observations and documents (Sanad, 2012). There are a number of reasons for not choosing this method for this research because this can offer no grounds for establishing reliability or generality of findings which cannot be reproduced or verified easily. On the other hand this research aim is to propose a framework for developing a DFC which should be reliable, general solution based on number of organisations not on a particular organisation.

3.3.3 Action Research

The action research methodology is learning by practicing method, in other words one only learns by doing the experiment or practice. The process of this methodology can be describes as a loop or circle process. This process goes through a number of major stages, first the definition of the problem, secondly make an effort to solve this problem, and finally evaluate the results if they are satisfactory, then the target is achieved and the loop stops, otherwise the process should be continued until a satisfactory result is achieved (O'Brien, 1998).Therefore this methodology cannot be used in this research as its aims are clearly to identify and document the stages and procedures taken by organisations in order to develop their DFC.

3.3.4 Ethnography

This method is used in observing the behaviour of people or cultures of people for example the employment of disabled persons in call centres. In technology this method is used to observe the human interaction with systems (Denscombe, 2007). Ethnography is capable to examine complex cultural phenomena. A common data collection for this method is the observation over period of time (Denscombe, 2007; Oates, 2006; Collis and Hussy, 2003). The restriction of this methodology is that the research should only focus on one specific group or person for a period of time and we aim in this study to involve a number of organisations. Moreover this research aims to develop a framework for building and managing DFC and such research method and results cannot be generalised, therefore this method cannot be used in this research.

3.3.5 Experimental

This method studies existing theory to make a prediction and design an experiment to test the prediction and then observe the experimental results (Oates, 2006). It can be used, create or modify the theory based on the experimental results. This method cannot be applied to this research as there are no standards/theories to develop DFC.

3.3.6 Narrative Research

This method studies a single individual and his life or the particular experience an individual through analysis of biographical data, text and semantic field analysis or reconstruction of the life history (Creswell, 2013). In another words narrative research depends on stories as told by others, for example: studying someone's experience as told by another person and not the person himself. This method cannot be applied to this research because it is looking at the behaviour of members from a number of organisations when taking decisions in developing DFC, therefore it is not wise to limit this research to the experience of an individual.

3.4 Justification for Research Strategy and Design Selection

According to Sekaran (2006), a researcher should consider the questions, aims and time constraints in the research, before choosing the appropriate research strategy. After considering the research questions, the aims of the research, in proposing a framework for DFC and the normal time constraints in the research, Grounded Theory, was identified as the most appropriate research strategy to employ.

Glaser & Strauss (1967) and Charmaz (2006) agree that grounded theory was primarily developed to serve and be applicable in social science research. Carlton (2006, 2007), Kessler (2010) and Hewling, (2013) used grounded theory in their research, which was in the field of DF.

The reason behind choosing grounded theory for this research is that the data collection methods in this theory are the most appropriate. More specifically the grounded theory which is a commonly used method in the interpretive paradigm, has been observed by Fernandez (2004) as being well suited in information technology research that involve social interactions between people using information technology or people's interactions with information technology. As mentioned in Chapter One, the researcher sought to identify, document and evaluate the stages and procedures followed by organisations in developing their DFC. The research at hand, therefore, deals with the interactions of DF investigators with digital evidence data, the interactions of DF investigators with others

involved in the DF environment, and the interactions of DF investigators with technology used in DF investigation.

Grounded theory has been employed in information technology literature since early 1990's and has been employed in research subjects ranging from software development, IT strategy, and the use of computer aided engineering software to effect organisational changes (Orlikowski, 1993). Furthermore, a computer system conference held in 2009 presented nine papers that applied grounded theory to information technology topics, thereby clearly establishing the relevance of grounded theory in the field. Moreover, grounded theory is useful for early studies of a new discipline and enables an examination of how people respond to various phenomena (Charmaz, 2006). Since DF is a new field of study, involving interactions between people and technology, grounded theory seems most appropriate in developing a framework for DFC (Carlton, 2006; Urquhart et al. 2010).

3.5 Data Collection Methods

After identifying the research strategy, the next step is to determine the appropriate data collection method (Robson, 2002). Grounded theory, as a research strategy, allows the use of various and sometimes multiple methods for data collection (Birks and Mills, 2011; Oates, 2006). The data collection techniques that a researcher may employ under grounded theory include (1) interview, (2) direct and participant observation, (3) content or documentary analysis, (4) focus group, and (5) survey.

3.5.1 Interviews

An interview has been defined as "an interaction between an interviewer and a respondent, from which the interviewer can infer whether the answers have relevance to the research questions" (Marshall and Rossman, 1999). Using this method one can collect the most relevant and credible data as this method involves person-to-person interaction. Interviews also help the interviewees to ask for an explanation to the questions they did not fully understand so that the researcher can clarify them, especially in a semi-structured interview setting which give the researcher the flexibility to use non-standardised questions. On the

other hand, in a structured interview, the researcher uses a standardised question which is ideal for a large number of participants (Denscombe, 2007).

Difficulty may arise transcribing the interview recordings but the researcher can overcome this by proper planning. There is an advantage of this kind of interview method that the researcher can assess/understand the candidate's knowledge level by observing their answers and their reactions to the questions. Other advantages to this interview method include a high rate of response from participants, flexibility, in-depth understanding of the phenomena, and the ability of the interviewer to probe the interviewee (Neuman, 2004). The disadvantages to the interview method are that it is time consuming, costly, and may be prone to interviewer's bias (Robson, 2002).

3.5.2 Direct and Participant Observation

Direct participant observation is the "process of gathering open-ended, first-hand information by observing people and places at a research site" (Creswell 2005, p.211). Using this method, the researcher collects large volume of data. Seeing and listening are the key factors in observation. Random visits to organisations and laboratories may be a more reliable indicator of whether people are using practices recommended than by simply asking people and making the data more reliable. Observing management operations in organisations may produce better information than relying on reports or key informants.

Direct observation is entirely different from participant observation. This method enables the researcher to observe possible sources of information i.e. physical settings of the DF laboratory and its environmental features, investigation reports, people and their behaviour, reactions and interests towards the development of DFC. It might be difficult to get access to some of the laboratories or organisations to carry out this method but this can be achieved by good contacts and interactions with the prominent people in the industry. Criticisms of this method are that it requires ample field time, can cause ethical issues for the researcher, and may be prone to observer bias.

3.5.3 Content or Documentary Analysis

Content analysis is one of the regularly used techniques because documents are often ready for analysis, assuming that are readily accessible and available (Stemler, 2001). This technique has three distinct approaches: conventional, directed and summative, and all three approaches deal with text data. Coding schemes, threats to trustworthiness and origins of codes are the most significant differences between mentioned approaches. In conventional content analysis, coding categories are derived directly from the text data. With a directed approach, analysis starts with a theory or relevant research findings as guidance for initial codes. A summative content analysis involves counting and comparisons, usually of keywords or content, followed by the interpretation of the underlying context. Documents may include minutes of meetings, policy and strategy documents, laboratory manuals, guidelines, letters, reports, web pages, and other useful documents (Marshall and Rossman, 2006).

5.3.4 Focus Group

Any focus group's method involves data collection method whereby the researcher invites a group of participants to discuss a research problem or a set of research questions (Yates, 2003). Researchers used the focus group method, for example, to verify research questions later to be used in other data collection methods like the interviews. In other words, a researcher may use the focus group to supplement the primary data collection method. The disadvantage of the focus group is that it could be costly and may be difficult to schedule (Bryman, 2008).

5.3.5 Survey or Questionnaire

Surveys or questionnaires are carried out to gather data not readily available in the literature (Remenyi and Williams 1998). The survey or questionnaire may be conducted in person, via telephone, email, or the use of websites. This includes request and study of specific information related to research. Construction of questions is important and there should not be leading or biased questions. The strength of this method is that a researcher can gather as much data from many people, saving time and money. The data can then be analysed using

a systematic method and researcher and any bias can be avoided. However, it also has some limitations such as the credibility or trustworthiness of the responses, limitations as to the length of the questions, and a low return rate of response (Denscombe, 2007; Neuman, 2004).

3.6 Justification for the Data Collection Method Selection

The primary data collection method in this research will be the semi-structured interview. First, the interview technique has been used by many researchers under Grounded Theory (Birks and Mills, 2011). Second, the interview method gives the researcher flexibility in understanding how a DFO and its processes operate. The comprehensive data derived from an in-depth interview is most appropriate to unmask the complexities of a new field of study such as DF. Third, the researcher most likely can obtain a high response rate with prolonged interaction in an interview setting. Furthermore, the researcher can likely be able to probe the participant with regards to questions, therefore allowing in-depth understanding of the processes, people, technology, and dynamics of a DF laboratory. Grounded theory interviews are specifically designed to draw out stories and free associations from the data collected (Charmaz, 2006; Glaser and Strauss, 1967).

Whenever possible, the researcher conducted the interview at the DF laboratory of the participant in order to supplement the interview with direct observation. The researcher should plan to record the interview in order to limit bias created by note taking (Charmaz, 2006; Robson, 2002).

Chapter Four: Planning and Designing Data Collection Process

4.1 Introduction

The aim of the research is to document, evaluate and analyse the stages and procedures taken by organisations in developing their DFC in the private and public sectors. Therefore, collecting data from different stakeholders in the private and public sector will indeed help the researcher to understand the procedures in depth to achieve the research aims. In the next section, the researcher explains the selection of organisations and the participants and ethical considerations related to the interview process.

4.2 Selecting the Organisations

It is important to identify the organisations between the public and private sectors to be selected were in order to have an in depth knowledge of how they developed their DFC. Private organisations are most likely to be investing in the latest technology and to specialise in specific fields of DF. Therefore, the selection of organisations in the private sector does not represent all of the private sector in the field of DF and hence selecting other organisations in the private sector will be explained in the next chapters. On the other hand, public sector organisations are considered to be investing to have solutions for different DF investigation scenarios.

The criteria that were used for selecting the sample were those organisations that engage in DF. A DF investigator, DF manager, DF laboratory owner or operator, DF director, DF sponsor, law enforcement officers and experts, DF academics, or DF expert freelancers, any from this list had to be available to participate in the interview within the different private and public sectors.

4.3 Ethical Considerations

The interviews were conducted after obtaining ethical approval from the University, especially as the research involves interaction with humans. The researcher did not encounter any ethical issues in the research project as the researcher obtained informed

consent from participants and safeguarded the participants' information through confidentiality safeguards.

4.4 Interview Protocol

The purpose of the interview protocol was to guide the researcher in the process of the data collection. Therefore, a protocol was prepared by the researcher before conducting interviews, which is explained in the table below. Each interview question was designed to achieve one of the crucial research aims see (cf. Section 1.3) by answering one of the six research questions (cf. Section 3.1.4) as shown in (Appendix 8).

Table below includes the purpose of the interview, general information about the interview, interview guidance and checklist. Examples of interview questions and glossary of terms are presented below.

1- Purpose of the Interview:

Identify patterns in establishing and managing DFOs with the ultimate aim of proposing a development framework for establishing and managing Digital Forensics Capability.

2- General Information about the Interview

Participant Name:	Organisation:	Role in the Organisation:
Place of the Interview:	Date of the Interview:	Duration of the Interview:
Language interview conducted :	Electronic Copy: YES / NO	

3- Interview check list:

• Introduce yourself + Shake hands + Exchange business cards	
• Inform the participant about the purpose of the interview	
• Show the participant letter from the University declaring the data is collected for research purposes	
• Ask the participant permission to record the interview with a digital recorder and taking notes during the interview	
• Inform the participant about the stages of the interview (Sections = 5 , No. of questions = 28 and duration = 60 minutes)	
• Give the participant consent form	
• Ask the participant if he has any questions	

• Start the questions and start the timer	
• At the end of the interview the researcher will summarise the interview session and thank the participant ask to contact you if he has more clarification regarding his answers	

3- Examples of Interview Questions

A - Background Questions:

1. How long you have been in the field of DF?
2. How long you have been in this organisation?
3. What is your field of study? (qualification)

B- Examples of Research Questions:

Question	Purpose	Expected answer
1-Guidelines and procedures (1-10)		
1. Do you know a guideline for developing DFO?	To determine if there is a guideline for developing DFO	No ,only available text book for building a managing a successful laboratory does not provide a framework but follows an informal list of factors for what the author believe what successful lab is
2. Do you know a guideline for managing DFOs?	To determine if there is a guideline for managing a DFO	No ,only available text book for building a managing a successful laboratory does not provide a framework but follows an informal list of factors for what the author believe what successful lab is
3. If there if is a guideline please provide the name or source?	To determine if there is a guideline for developing or managing a DFO, which is the	None

	research problem?	
4. Do you follow any such guideline?	To see how Widely the guideline is used	No
5. How did you establish your organisation? Can you identify steps taken to develop your DFO or facility?	To determine or identify pattern that DF orgs use in developing DF orgs	-Establish key HR positions -purchase key hardware and software -develop key policies to govern access to facilities

At the End of Interview:

Thank the participant and ask if he/she has any final comment that they feel will add value to the research and was not asked by the researcher?

Glossary of Terms:

Digital Forensic Organisation: a social unit of people engaged in DF that are structured and managed to meet a need or to pursue collective goals that are related to DF. This organisation can also be referred to the social unit engaged with DF Laboratory

Facility: a place, amenity, or piece of equipment provided for a particular purpose (Oxford Dictionary, 2013)

Capability: the power or ability to do something (Oxford Dictionary, 2013)

Digital Forensic Capability: the ability to establish and manage Digital Forensic Facility with proper staffing, training, selecting tools and providing managerial framework

Guideline: a general rule, principle, or piece of advice: i.e. the organization has issued guidelines for people working with prisoners (Oxford Dictionary, 2013)

Framework: a basic structure underlying a system, concept, or text. i.e. the theoretical framework of political sociology (Oxford Dictionary, 2013)

Table 1 Interview Protocol

The researcher started the data collection through the use of a pilot study to refine further the interview questions and timing of each session, and as a result the interview questions were modified. The next section shows in detail how the pilot study was conducted and the data collection process carried out. In addition to the justification for choosing the candidates and organisations, ethical issues related to the interviews and the protocol followed in such data collection method and is explained.

4.5 Pilot Study

Since the focus of this research is on different types of digital forensic organisations (Public and Private) and in two countries (the UK and the UAE), the author decided to start with a private digital forensic organisation; the Blackstage Forensics Limited for the pilot study. One interview was conducted with the managing director of the company. The researcher used the initial questions proposed in the methodology chapter, and the interview took place in the interviewee's workplace during working hours.

Grounded theory methodology usually starts with open-ended questions to obtain in-depth and relevant information on the research questions. Therefore, a series of semi-structured interviews were conducted, affording the informants the opportunity of supplying their opinions, knowledge and experience on a wide range of issues in an attempt to explore and answer research questions left unanswered in the literature review. The questions were divided into five main areas covering (1) guidelines and procedures, (2) infrastructure, (3) organisational policies, (4) human resources, and (5) investigation processes. The interview consisted of a total number of 29 questions. A total of 2 interviews were conducted for the pilot study and the proposed time for each interview session was 60 minutes.

4.5.1 Introduction to Pilot Study

The sections below discuss the planning and execution of the pilot study as follows. Section 4.5.2 covers the planning of the pilot study. Sections 4.5.3 and 4.5.4 discuss the selection of interviewees for the pilot study. Section 4.5.5 presents the backgrounds of the participants and organisations they belong to, including the justification for choosing the interviewees for the pilot study. Section 4.5.6 explains the ethical considerations for the

pilot study. Sections 4.5.7 and 4.4.8 discuss the execution of the pilot study. Section 4.4.8 discusses data analysis and provides an example. Section 4.5.9 shows questions modified and finally 4.5.10 discuss lessons learned from the pilot study and conclusion.

4.5.2 Planning of the Pilot Study Data Collection Process

The aim of the research is to study existing developmental frameworks for establishing and managing DFC. In order to support the outcomes of the research aims, the researcher gathered qualitative data by conducting interviews with various stakeholders in the field of DF. Data were gathered using interviews of individuals in private and public organisations in the field of DF in both the UAE and the UK.

Before proceeding with the full empirical research data collection process, it is important to conduct a pilot study to make sure that the data collection instruments are reliable, putative problems considered and addressed, and whether the data collection instruments support the data analysis and inform research analysis and research questions. This chapter explains the pilot study, initial data collection process and the lessons learned from the pilot study to improve the research methodology.

4.5.3 Design of the Data Collection Instruments and Documentation

The data collection instruments and documentation have been designed paying due regard to ethical research practices and Grounded Theory (Yin, 2009; Charmaz, 2006; Glaser and Strauss, 1967). Semi-structured interviews were used in this research, because interviews have been the main source and primary technique for data gathering in Grounded Theory methodology by many researchers (Birks and Mills, 2011; Yin, 2009; Corbin and Strauss, 2008; Allan, 2003; Walsham, 1995).

The semi-structured interview is flexible, yet the researcher can derive rich data and can uncover the complexities of a new field of study such as DF. The researcher will also likely obtain a high response rate from the interviewee through prolonged interaction in an

interview setting. The researcher estimated that each interview session should last approximately one hour.

As Grounded Theory interviews are specifically designed to draw out stories and free associations (Charmaz, 2006; Glaser and Strauss, 1967), the researcher was also able to probe the interviewee, allowing in-depth understanding of the processes establishing and managing digital forensic provisions, people, technology, and dynamics of a DF provisions. In particular, the researcher developed the interview protocol to support the researcher in the process of the data collection. The interview protocol includes the purpose of the interview, general information about the interview, interview guide line and checklist, interview questions and a glossary of terms. Furthermore, the interview questions are divided into five main sections: Guidelines and Procedures, Infrastructure, Organisational Policies, Human Resources and Investigation Process with a total of 29 questions.

4.5.4 Selection of Interviewees for the Pilot Study

The participants for this research were selected and they were not random. The sampling followed Grounded Theory because participants were selected using purposive sampling, which means that the selection criteria were based on who the researcher deems is a typical participant or of interest for the research (Robson, 2002). Purposive sampling is consistent with theoretical sampling under Grounded Theory, which is unlike the traditional sampling that gathers a representative population and which is used in other types of qualitative and quantitative research (Charmaz, 2006; Robson, 2002).

There are two types of service providers in the field of DF: public and private organisations. In order to get a comprehensive view, it is important to get data and insights from both the public and private sector. The pilot study focused on interviewing the private sector because (1) private entities showed a strong interest in participating in the pilot study, and (2) there are more private sector DFOs than public sector organisations.

The researcher conducted the pilot study in two countries: in the United Arab Emirates and in the United Kingdom. The two private organisations were chosen, Contego Solutions (UAE) and Blackstage Forensics Limited (UK).

The researcher found Contego Solutions as a candidate after conducting extensive online research, and the organisation was contacted and invited to participate in the pilot study via email. On the other hand, Blackstage Forensics Limited was introduced to the researcher through an informal meeting, and the interview was arranged thereafter.

4.5.5 Background of interviewee's organisations

4.5.5.1 Contego Solutions

Contego Solutions has its main headquarter in Germany with a branch in the UAE, among other places. Contego specialises in "high technology fields of DF, Data Centre Installation, Professional Services, and System Integration" (Contego, 2016). It has clients ranging from public and private organisations in the MENA (Middle East and Northern Africa) region and the APAC (Asia Pacific) region. Contego has been in the market for the past four decades (Contego, 2016).

4.5.5.2 Blackstage Forensics Limited

Blackstage Forensics Limited is based in Derbyshire, United Kingdom. The organisation is a small enterprise managed by David Benford, who is an "internationally renowned cybercrime expert, specialising in risks derived from social media, the Internet, geo-locational data and in risks from how we use portable digital devices" (Blackstage, 2106). Blackstage is involved in training both public and private clients in law enforcement and business. Blackstage has also worked with law enforcement agencies in South East Asia and Europe, including the training of diplomats in Brussels (Blackstage, 2016).

4.5.6 Ethical Considerations

Ethical approval was obtained prior to conducting the pilot study (See Appendix 1). However, the researcher is aware that ethical approval is part of an ongoing process. The

ethical approval was granted after the researcher developed (1) research instrument, protocol and participation procedures (See Appendix 3), (2) consent form, and (3) agreement to participate (See Appendix 4). The researcher followed the Ethical Review Procedures of De Montfort University (De Montfort University, 2014) in conducting the pilot study, and asked the interviewees to read the "Overview and Agreement to Participate in Digital Forensics Research Study" (See Appendix 5) and the letter from my supervisor regarding the research (See Appendix 2). The interviewees were also asked to sign the consent form prior to the interview.

4.5.7 Execution of the Pilot Study

The researcher followed the formalities regarding the arrangement of the interviews with Contego and Blackstage, as discussed below. According to Denscombe (2007), the researcher has the responsibilities of obtaining the required approval for the interview and arranging the meeting's agenda, time and location prior to the interview. The researcher aimed to accomplish these responsibilities well ahead of time.

4.5.7.1 Interview with Contego Solutions, Director of Business Development

The interview with Contego Solutions' Director of Business Management was conducted in Dubai, UAE at the office of Contego Solutions in the Loft Building, Dubai Media City, on the 08th Dec 2013. The interview, as designed in the protocol to last one hour, met the time target in that it lasted exactly 58 minutes. The entire session, however, lasted longer than one hour due to the interest of the interviewee, who was keen to know more about the research in the field of DF. This informal discussion of DF topics was seen as useful by the researcher with the potential for relationship building and to allow for greater ease for follow up appointments.

The interviewee did not sign the consent form right away, as the interviewee explained that permission was required from his manager before signing the consent form. The interview had been scheduled ten days before the interview. The interviewee's organisation asked for a copy of the questions before the interview; however, a copy of the question was not

provided because awareness of the questions before interview was considered that it might lead to bias and defeat the purpose of a semi-structured Grounded Theory interview. The interviewee promised that later he would email the signed consent form, which he did. Prior to receiving the signed consent form, the researcher did not transcribe the interview or use the interview data. The researcher subsequently found out from the interviewee that a copy of the questions was requested to allow them to choose the right person to participate in the interview.

This experience gave the researcher opportunity to improve the research procedures. In future interviews, if an interviewee would like to view the questions prior to signing the consent form, the researcher will emphasise to the interviewee that answering any questions may have negative effects and that the interviewee may stop and withdraw from the interview at any time. This information was added in the email sent to the interviewee asking them to participate in the interview, and if necessary was repeated to reassure the interviewee.

Permission was obtained to audio record the interview before commencing the interview which was done for all interviews. An audio recorder was used during the interview and the interviewer also took the handwritten notes. The audio recording and taking notes during the interview are useful tools that researchers have successfully used at every interview (Leedy & Ormrod, 2010; Dick, 2005; Charmaz, 2000). According to Kessler (2010) “As data are gathered, the researcher takes notes of emerging themes”. The notes taken by the researcher will be kept in a secured place and destroyed after ten years after the pursuant to the ethical procedures of De Montfort University (De Montfort University, 2014).

The interview started in the meeting room of Contego Solutions at 3pm after the lunch break. It was a quiet place without any noticeable distractions before, during, and after the interview. It was an ideal atmosphere for an interview. Before the interview began, the researcher introduced himself and gave a business card, and the interviewee did likewise.

The interviewer began the interview by asking about the interviewee's background and informal questions. Then, the interviewer followed the protocol.

4.5.7.2 Interview with Blackstage Forensics Limited, Managing Director

The interview with the Managing Director of Blackstage Forensics Limited was conducted in Derbyshire, UK at the office of Blackstage Forensics Limited in the Old Stable, Catton Hall. The interview finished twelve minutes earlier than expected, which was one hour. One reason was that the interviewer has already met the interviewee informally before the formal interview, and therefore the introductions were shorter.

The interview had been organised more than one month before the interview took place. Permission was obtained to audio record the interview before commencing the interview and during the interview handwritten notes were also taken.

The interviewee signed the consent form straight away before commencing the interview. The meeting took place in a quiet location, at 10am, and there was no major disturbance before, during, and after the interview. Before the interview began, the researcher introduced himself and gave a business card. The interviewer began the interview by asking about the interviewee's background and then, the interviewer followed the protocol.

4.5.8 Data Analysis: Note Taking, Coding, Memoing

The data obtained from the Pilot Study interviews were analysed using Grounded Theory data analysis procedures, following the Straussian approach (Corbin and Strauss, 2008; Hekkala, 2007; Strauss and Corbin, 1998; Strauss and Corbin, 1990;). The Straussian methodology allows reviewing certain literature before starting the data analysis (Corbin and Strauss, 2008), similarly, in this research a literature was reviewed at start.), on the other hand the Glasserian methodology criticised reviewing the literature before data analysis to let the data speak for themselves and reviewing literature will discourage the coding and labelling of the data (Glaser, 1992; Glaser and Strauss, 1967). The data analysis in this research follows the Straussian approach because literature had been reviewed at the

beginning of the research, and also because the Straussian approach is common in the IS field (Hekkala, 2007). According to Straussian approach to Grounded Theory, the coding paradigm model for analysing data requires note taking, coding, and memoing (Charmaz, 2006; Strauss and Corbin, 1998). In note taking, the researcher must take notes of emerging themes, which is part of the data analysis, because it is made after the interview and with constant comparison (Charmaz, 2006; Pogson et al., 2002).

Constant comparison was also used during coding (Charmaz, 2006). Coding in Grounded Theory is defined as the "analytical processes through which data are fractured, conceptualised, and integrated to form theory" (Strauss and Corbin, 1998). There are three stages in the coding process: open ended coding, axial coding, and selective coding (Robson, 2002). In open-ended coding, the aim is to define simple categories and concepts for comparison and understanding (Robson, 2002; Charmaz, 2000). Corbin and Strauss defined concepts as "Words that stand for groups or classes of objects, events and actions that share some major common property(ies), though the property(ies) can vary dimensionally" (Corbin and Strauss 2008, p. 45).

The researcher must remain opened to possibilities and let the data lead. Axial coding narrows the focus by examining the data and providing a context for relationships in the data (Robson, 2002; Charmaz, 2000). Finally, according to Strauss and Corbin, selective coding is "the process of integrating and refining the theory" (Strauss and Corbin 1998, p. 143).

Lastly, data analysis in Grounded Theory requires memoing, where the researcher will arrange the trends to define categories and relationships and writing the observed trends into a theory (Dick, 2005; Charmaz, 2000).

The researcher took notes during the interviews, to keep track of emerging trends. This was especially important in the second interview, where the researcher observed differences between this and the first interview. After the interviews were transcribed, the researcher

categorised answers to questions for open coding, following the Straussian coding model paradigm (Corbin and Strauss, 2008; Strauss and Corbin, 1998; Strauss and Corbin, 1990). For example, the first question was about guidelines and one of the interviewees to whom the researcher assigned a Facetted code (01BLINTUK13, which means First interview, Blackstage, Interview, United Kingdom, 2013), gave an answer which stated "making sure that I got my own sense of ethics and rules." This answer was open coded by researcher under "Ethics." This categorisation is consistent with the open-ended coding in Straussian approach to Grounded Theory (Corbin and Strauss, 2008; Strauss and Corbin, 1998; Strauss and Corbin, 1990). The answer by the interviewees under this category was then placed into categories based on the researcher's predetermined categories. The subcategory of "Ethics" was placed under the category of "Guidelines" and under "Organisational Policies." The arrangement of codes into categories and subcategories follows axial coding under Grounded Theory according to the Straussian approach (Corbin and Strauss, 2008; Strauss and Corbin, 1990; Strauss and Corbin, 1998). Finally, in axial coding, the data were then coded according to how they matched the aims of the research relating to guidelines and organisational policies (Corbin and Strauss, 2008; Strauss and Corbin, 1998; Strauss and Corbin, 1990). The researcher can then create theories based on the systematic categorisation of the data.

4.5.8.1 Example of Data Analysis

1. **Open Coding**

The aim of this research was to study existing DFOs in order to see what recommendations exist with regards to developing DFC. In addition, how widely these recommendations are used to identify patterns in developing DFC. Furthermore, this research aims to explore whether organisations use guidelines or standards for managing their capability.

In this section, the researcher provides an example of data analysed from the interviews and then identified emerged codes step by step. The researcher labelled a number of texts via underlining as potential items representing codes or concepts. By reviewing underlined keywords in the answer of the participant (02CONINTUAE13), a number of codes

emerged, for example (guideline, recommended practices, vendors, ISO standard and organisation need). This line by line approach follows the Straussian coding model paradigm (Corbin and Strauss, 2008), which suggests reviewing the excerpt line by line. From this approach, the participant response suggests that there is no set of standard guideline for developing DFC.

1. While analysing the second participant's (02CONTINTAE13) answers, other codes emerged and concepts were identified such as guideline, setting up companies, setting up my own company, ethics etc. Ethics was identified as a concept, which shows that the participant did not follow a guideline for developing DFC; however he treated DFC as a commercial company, and used his sense of ethics as a substitute to guidelines. The identification of concepts follows the Straussian coding model paradigm (Corbin and Strauss, 2008), as described above following Corbin and Strauss' definition of concepts.

2. Then, the concepts were grouped into categories. Categorisation is the next step in the Straussian coding model paradigm, which encouraged the generation of initial categories (Corbin and Strauss, 2008; Strauss and Corbin, 1990). The researcher discovered that concepts such as standard, ISO standard, guideline and best practices, share similar properties and therefore they were grouped into one category **Guidelines and Procedures**. Similarly creating company, organisation need and vendors share similar properties and therefore they were grouped into **Infrastructure**. In addition, to the concept of Ethics and conflict of interest share similar properties and were grouped as **Organisation polices**. Furthermore all issues related to the personnel in DF such as Training, certification and education share similar property from an organisational perspective and were therefore grouped as **Human Resources**. Finally, all issues related to investigation process such as rules of evidence, chain of custody, logging all information, secure evidence share similar properties and were grouped as **Investigation Process.**

2. Axial Coding:

Axial coding comes after identifying categories in the open coding process by finding relationship between the categories. Axial coding is the next step in the Straussian coding model paradigm, which defined axial coding as the "process of relating categories to their subcategories" (Corbin and Strauss, 2008; Strauss and Corbin, 1998, p. 123).

1- The "Guideline and procedures" category was found to have an impact on the "organisation policies" category. This relationship was identified when the participant said "But it was just the case of creating my own company and making sure that I got my own sense of ethics and rules". This example shows that the participant used his sense of Ethics and Rules as a substitute for guidelines and procedure to establish his company.

2- "Guideline and procedures" was also found to have an impact on the "infrastructure" category. This relationship was identified when participants said "it was the case of creating my own company" and the other participant said "Depending on organisation need". This is a casual relationship due to a lack of standard infrastructure building in DFC.

3- "Guideline and procedures" were also found to have an impact on the "Investigation Process". This relationship was identified when there was no standard documented process for investigation when participant said "as long as you do acquisition and analysis …. follow the rules of evidence, you know the chain of custody, you have the secure…basically, the capability to secure evidence, and to log in all the information, then that's fine, that should be okay" .

3. Selective Coding:

Selective coding is the final step in the data analysis process. Corbin and Strauss defined selective coding as the "process of integrating and refining the theory" (Strauss and Corbin 1998, p. 143). Following the Straussian coding model paradigm, all categories in the data are inspected in order to find the main category and central phenomena which it might be in this research (standard guideline or minimum requirement) which are abstract and related to all categories. From the above, a number of theories can be generated, for example:

-Existing DFOs lack standard guideline for establishing DFC, which made the participant to use his sense of Ethics as a substitute.

- Exploration of how a number of organisations develop their DFC and whether they used any guideline. From participants' answers, we identify a pattern that did not follow a specific guideline to establish their capability.

4.5.9 Interview Questions modified

This section shows as to which questions have been altered or modified in the interview question list: (a) question number 11(shown in the table below) was modified to include four follow up questions and an additional fifth question about the use of open source tools. This modification was added because one of the aims of this research is to find out how do organisations select their tools. These added questions helped to identify the way organisations select their tools for investigation process.

Question	Purpose of the question	Expected answer
11. What are you commonly used tools in DF lab (Hardware and Software)	To identify a standard pattern for DF capability, process and tools in private or public organisations	According to the crimes, situation or scenario which requires investigation. EnCase and FTK could be the strongest candidates.

Table 2 Interview Question No.11 before Modification

11. What are your commonly used tools in DF lab (Hardware and Software)	To identify a standard pattern for DF capability, process and tools in private or public organisations	According to the crimes, situation or scenario which requires investigation. EnCase and FTK could be the strongest candidates.
• What is the reason behind using this particular software? • Is this due to business requirement? • Is it because of the efficiency of these products? • Or is it for financial reasons?	To identify the reason behind choosing specific tool or software	According to the business need and finical capability
• Do you consider using open source tools and why?	To see how widely free tools are used and reliable	Yes to verify investigation results

Table 3 Interview Question No.11 after Modification

(b) Question number 24 was also modified by adding three follow up questions as shown in the table below. This modification was made because one of the aims of this research is to identify and document the training requirements for different forensic practitioners in a range of organizations, particularly with regard to CPD (Continuing Professional Development). This modification ensured the identification of the minimum requirement for qualifications in the field of DF. In addition, this modification also helped to determine the type of training people require in the field. Finally, helped to identify how experience in the field of DF is determined.

24. How do you become a digital forensic investigator? What are the needed qualifications, training, or experience?	To determine the minimum requirement/qualification for a DF investigator	Based on experience and training

Table 4 Interview Question No.24 before Modification

24. How do you become a digital forensic investigator? • Do you require a particular qualification to become a DF investigator? • Do you require a particular training for executing DF investigation? • How long experience do I need to become a DF investigator? And is there a particular field to work in?	- To determine the minimum requirement/qualification for a DF investigator - To determine if there is particular certification or experience required to become an investigator - To determine if there is a pattern in qualifying a DF investigator	- Computer security - The training is based on the business requirement

Table 5 Interview Question No.24 after Modification

4.5.10 Procedural, substantive, and strategic lessons learned from the Pilot Study

The lessons learned in the pilot study interviews with regards to improving the interview procedures, interview substantive questions, and interview strategies is addressed in this section. The interview protocol helped the process of the interview. The researcher has followed the steps in the protocol, which was designed specifically to conduct these interviews. The exchange of the business cards in the interview protocol helped engage the candidate more in the interview especially after showing that this programme is funded by the Dubai Police and the researcher is a senior police officer.

Issues Raised

(1) The researcher created a chart of each of the questions used in the pilot study with corresponding answers (See Appendix 8). The chart shows that each question generated answers from the participants and the answers provided sufficient data for analysis using Grounded Theory. There were instances where the answer to a question was shorter but this occurred in questions 3 and 4 because these questions were follow up questions intended to verify an answer and where the interviewee

was asked to provide a specific source. Also, there were times when the interviewee had already answered a question in a previous question, so the answer to the question might not appear immediately in the transcript. Overall, a reviewing the chart of questions confirmed that the interview questions were effective in analysing data.

(2) Participants also did not ask for clarification on the questions during the interview, which suggests that the interview questions were clear and easy to understand and answer.

(3) The researcher also found that the interview questions supported the research aims and the research questions. First, the researcher had matched the purpose of the interview questions with the aims of the research. The researcher created a chart that shows the questions, the aims of the research and expected answer. Second, the expected answers were met for most of the questions, but some questions were not answered as expected. Examples of questions that did not produce the expected answer were Questions 6, Question 8, Question 24, Question 27, and Question 29. The different outcome of the answers in these questions, however, does not reduce the reliability of the data and their usefulness in answers the research questions. Consistent with Grounded Theory, the answers to the questions allow for more data to lead the research and inform the researcher as more interviews were conducted.

(4) In the guidelines and procedures section of the interview, both interview candidates suggest that there is no standard guideline or a framework in order to establish or manage a DFC. Instead the available recommendation with regard to establishing and managing DFC is either from vendors or best practices shared by organisations. In addition question 9 needs to be more specific to identify minimum factors to make the organisation capable for digital forensic investigation.

(5) The questions explored more about the infrastructure of the digital forensic organisation. Both candidates gave similar answers to the majority of the questions in the infrastructure section. For example, both interviewees stated that their organisation use EnCase and FTK as hard drive analysis software, that their

organisation also did not use the “cloud” as a platform for their operations, and neither candidate’s laboratories or organisation have any ISO accreditation.

(6) Questions were designed to explore policies and procedures in digital forensic organisations. The candidates did not provide specific answers to the questions regarding the policies and procedures in place in their organisation. In other words, both interviewees tried explaining the existence of policies in their organisation governing their DF environment by giving examples, but neither interviewee provided me with a written policy and procedure governing their organisation.

(7) Questions that were designed to discuss human resources in the digital forensic organisations. Interestingly, none of the candidates mentioned a particular qualification or certification that the digital forensic investigator must hold and both agreed that a digital forensic investigator must maintain regular training between 1-3 courses each year.

(8) The question related to investigative tools was found to require follow up questions to clarify the answers given by the candidates and to give more support to the research questions by obtaining in depth answers. Therefore, follow up questions were added as described Section 4.5.9 above.

(9) The question related to personnel training and experience was found to require follow up questions to clarify specific training requirements and specific experiences that candidates required. This allowed the researcher to compare with existing literature on training requirements and to obtain more in depth data to support the research questions. The follow up questions identified can be seen in Section 4.5.9 above.

(10) The pilot study was also a learning point for how to do the data analysis, and it allowed the researcher to test the data analysis used by Grounded Theory, which is new in the DF field. The researcher learned specifically how to do the open coding, axial coding, and selective coding by applying the procedure to the pilot study data.

Finally, being familiar with the interviewee is helpful because it saves time in the introduction and conducts the interview more at ease.

4.6 Planning and data collection process

This section discusses the re-planning of the data collection process from interviews. Section 4.6.1 reviews the lessons learned from the pilot study. Section 4.6.2 covers the design and planning of the data collection. Sections 4.6.3 discuss the interview participants and the organisations, including the selection of the participants.

4.6.1 Lessons from the Pilot Study: Finalising the Data Collection

Before proceeding with data collection, it is important to apply the lesson learned from the pilot study consider them as a basis for the data collection process. The guidelines from the pilot study are as follows:

(1) The researcher will use the interview protocol used in the pilot study as it has proven its effectiveness (See Appendix 3).
(2) The researcher will use interviews to collect data (cf. Chapter 4.5.10).
(3) The pilot study confirmed that questions were clear for the participants; however two questions (Question 11 and Question 24) were modified to solicit more in-depth answers.
(4) In Question 9, the researcher will seek more specific answers rather than general answers.
(5) The pilot study shows that further modification of the questions may be required due to constant comparison, which is part of grounded theory.
(6) The researcher will use the Straussian approach of Grounded Theory for the data collection and data analysis with the use of coding model paradigm (Strauss and Corbin, 2008).

4.6.2 The Design and Planning of the Data Collection

The aim of the research is to study existing developmental frameworks for establishing and managing DFC. In order to support the research aims, the researcher gathered qualitative data by conducting interviews with various stakeholders in the field of DF. Data gathered from the interviewees in private and public organisations in the field of DF in both the countries, UAE and the UK.

4.6.2.1 Type of Interview: Semi Structured Interview

The pilot study confirms that the semi-structured interview is the most appropriate research method for data collection according to Grounded Theory and as demonstrated and explained in the pilot study (cf. Section 4.5) (Birks and Mills, 2011; Yin, 2009; Corbin and Strauss, 2008; Allan, 2003; Walsham, 1995). The advantages of the semi-structured interview as discussed in chapter 4 are that it has proven to collect sufficient in-depth data during the pilot study because the response rate was 100% in the interviews and every question was answered (cf. Chapter 4). Grounded Theory interviews are specifically designed to draw out stories and free associations (Charmaz, 2006; Glaser and Strauss, 1967). The rich data will therefore likely uncover the complexities of a new field of study such as DF.

4.6.2.2 Scheduling of Interviews

Designation	Organisation	Year	Country
1. Managing Director	Athena Lab	2014	UAE
2. Professor	UAE American University	2014	UAE
3. Consultant	Private Sector Investigator & trainer	2014	UK
4. Consultant	Private Sector Investigator & trainer	2014	UK
5. Head of Technical	Contego Solutions	2014	UAE
6. Manager- Information Security Protection	StarLink	2014	UAE
7. Principal Consultant	Mandiant	2014	UAE
8. Senior Security Researcher	Kaspersky	2014	UAE
9. Project Manager -UAE Centre of Digital Innovation	Telecommunication Regulatory Authority - UAE	2014	UAE

10. Junior Digital Forensic Investigator	Telecommunication Regulatory Authority -UAE	2014	UAE
11. Director of Cyber Security & Investigation Services	Nuix	2014	UK
12. Managing Director	Evidence Talks	2014	UK
13. Visiting Professor- Managing Director at	4N6 Investigation Ltd.	2014	UK
14. Senior Hi Tech Officer	West Yorkshire Police	2014	UK
15. Technical of Cyber Crime Consulting Foundstone	McAfee	2015	UAE
16. Director & Head of Forensic Technology	Deloitte	2015	UAE
17. Director	Deloitte	2015	UAE

Table 6 Empirical Research Participants

4.6.3 Interview Participants

Following Grounded Theory, as discussed in Chapter 4 (cf. Section 4.6), participants were selected using purposive sampling (Robson, 2002). They were selected from both, public and private sector organisations following the lessons learnt from the pilot study. In order to get a comprehensive view, it was important to get data and insights from stakeholders. The researcher conducted the data collection in two countries: the United Arab Emirates and the United Kingdom and the following sections shows participants backgrounds and their organisations

4.6.3.1 Athena Laboratory

Athena laboratory is a private company located in Dubai, UAE, specialising in DF and Security Solutions (SS). It's founder, Mr Asif Iqbal, is a consultant of DF and SS for over 16 years' experience in Disaster Recovery, Risk Management, ISO27001, CobiT, ISO20000, DF investigations, Fraud Investigations and Audit and their implementations.

Mr Iqbal is also a member of IEEE, ACM, ISACA, ACFE, ISC2, PMI, and ASQ and has certificates of CISSP, CISA, CISM, CGEIT, CFE, CobiT, ISO20000 and ITIL. Athena Laboratory is heavily involved in research and development and their experiments make use of the latest gadgets such as google glass, smart TV's and the kindle fire (Athena-Labs, 2016).

4.6.3.2 UAE American University

The UAE American University was established in 2006 in Dubai Academic City, Dubai, UAE; it is known as the AUE. AUE is a private university approved by the Ministry of Higher Education and Scientific Research and is licensed by the Commission of Academic Accreditation. AUE offers wide range of courses at both, undergraduate and postgraduate levels and has partnerships with a number of academic, non-academic and corporate institutions and organizations around the world. AUE has DF Laboratory and master degree program in Enterprise Security and Assurance with in-depth material of information security and digital forensic theories and techniques (The American University in the Emirates, 2016).

4.6.3.3 StarLink Limited

StarLink Limited is one of the fastest growing IT security solution companies across the Middle East, with branches located in 10 different countries. It is recognized as a "Trusted Security Advisor" to over 1000 enterprises and government customers that use one or more of StarLink's technologies (StarLink, 2016).

4.6.3.4 Mandiant

Mandiant is a cyber-security company which was established in the USA in 2004. It offers urgent incident response services and non-urgent general security consultations to major international organizations and governments. In December 2013, it was taken over in a $1 billion deal by a company called FireEye. This security company is a well-known by its regular cybersecurity report through its intelligent centre (Mandiant, 2016).

4.6.3.5 Kaspersky

Kaspersky is a private cyber-security company founded in 1997 in Russia. It is considered to be one of the fastest growing companies with branches in 31 countries and providing services in 200 countries. The company's revenue in 2014 exceeded $700 million and it has more than 3000 qualified staff. This company is one of the leading cybersecurity solution vendors all over the world offering a wide a range of services and products such as Kaspersky Anti-Virus, Kaspersky Internet Security and Kaspersky Security for Business (Kaspersky, 2016).

4.6.3.6 Telecommunication Regulatory Authority – UAE

The Telecommunication Regulatory Authority (TRA) is a government agency which was established in 2003 to regulate the Information Communications and Telecommunications (ICT) sector in the UAE. The TRA to achieve its objective it has established the aeCERT in 2008 to enhance quality of information security practice standards. TRA is committed to provide a safer cyber space for the end users and corporates in the UAE through many initiatives within aeCERT. For example aeCERT provides a number of services to the community and corporates through awareness, education, monitoring and response. Besides these services, aeCERT more specifically conducts DF investigations (Computer and mobiles forensics) when needed for the monitoring and response purposes (TRA, 2016).

4.6.3.7 Nuix

Nuix is an Australian company in computer software industry, which was started by a fund from the Australian government in one of the universities in Australia. Nuix provides many services such as eDiscovery Tools, Digital Forensics Investigation Software, Big Data Management, Litigation Support, Risk Management, Cybersecurity and Incident Response. Nuix software is becoming one of the most popular tools in the field of DF and eDiscovery and Nuix products are being used by organisations in 45 countries. Nuix is famous for dealing with large amount of unstructured data and present them in more user friendly manner (Nuix, 2016).

4.6.3.8 Evidence Talks

Evidence Talks, established in 1993, is one of the UK's leading forensic computing companies. Since the beginning Evidence Talks has successfully been providing services to a wide range of organisations in both the private and the public sectors including the military and law enforcement. Remote Forensics and SPEKTOR Forensic Intelligence are the two award winning technologies which were developed in house in Evidence Talks laboratories, in addition to many other computer forensics technologies (Evidence Talks, 2016).

4.6.3.9 West Yorkshire Police

West Yorkshire Police, established in 1974, currently serving about 2.2 million people in Bradford, Calderdale, Kirklees, Leeds and Wakefield. Its Hi Tech crime division deals with a number of crimes on a daily basis. Its Hi Tech team conducts mobile and computer forensics investigations using various tools including EnCase, FTK and XRY. In addition, if required, the Hi Tech Crime can be presented in the court as expert witnesses (West Yorkshire Police, 2016).

4.6.3.10 McAfee

McAfee, established in 1987 is an international computer security software company based in the USA. It can be considered as one of the world's largest computer and internet security solution companies. In 2011 Intel Security took over McAfee to become one of Intel's entities to provide a wide range of services such as Data Protection, Database Security, Email & Web Security, Mobile Security, Network Security, Risk & Compliance. In addition, McAfee has developed a number of solutions for end users personal computer and internet security and corporate security needs. Examples are, McAfee LiveSafe, McAfee Internet Security and McAfee Antivirus (McAfee,2016).

4.6.3.11 Deloitte

Deloitte is a multinational professional services firm headquartered in New York City in the United States. It is one of the "Big Four" companies and the largest professional

services network in the world by revenue in financial year 2014 and the largest by the number of professionals. Deloitte provides audit, tax, consulting, enterprise risk and financial advisory services with more than 225,400 professionals in over 150 countries. The company currently has a total of 46 global member firms and in finical year 2015, earned a record $35.2 billion USD in revenues. As per reports in 2012, Deloitte had the largest number of clients amongst FTSE 250 companies in the UK and in 2015, Deloitte showed the highest market share in auditing among the top 500 companies in India (Deloitte, 2016).

4.6.4 Selection of the Participants

The sample size is in total 19 participants, 2 participated in the pilot study and 17 participated in the empirical research, which was determined using purposive sampling. In grounded theory research, the most commonly used samples are purposive (Robson, 2002; Miles and Huberman 1994). Grounded theory requires that the size of purposive samples ought to be established inductively and sampling should continue until "theoretical saturation" occurs (Guest et al. 2006; Robson, 2002). The problem with the purposive sampling approach, however, is that "guidelines for research proposals and protocols often require stating up front the number of participants to be involved in a study" (Guest et al. 2006; Cheek 2000). Therefore, the sample size is required as a general measure as to when theoretical saturation occurs (Guest et al. 2006).

A review of literature that provide guidelines for sample sizes in grounded theory study shows that in some cases six to twelve interviews are needed to reach theoretical saturation (Guest et al. 2006). Creswell (1998) suggested twenty to thirty participants for a grounded theory study. However, Creswell (1998) and other research did not give a general, numeric guideline as to what number range is needed to reach theoretical saturation. Mason (2010) conducted a study that showed twenty to thirty interviews are the most common size for a sample.

Guest et al. (2006) identified a general, numerical guideline as to the size of a sample needed to reach theoretical saturation in a grounded theory research that used non-

probabilistic and purposive sampling. While Guest et al. (2006) did not deal with DF research; their recommendation for reaching theoretical saturation for purposive sampling is nevertheless applicable at any number of samples. Guest et al. (2006) showed in their study that six to twelve interviews will generally be sufficient to reach theoretical saturation. Nielsen and Landauer (1993) found that saturation often occurs at the early stage of the coding, and theme or theory identifying process. The proposed sample size of 17 interviews is therefore, reasonable for initial data collection and analysis in this research.

4.7 Ethical Considerations

Ethical approval was obtained prior to conducting the interviews (Appendix 1). However, the researcher is aware that ethical approval is an ongoing process. The researcher worked in accordance with the ethical review procedures of De Montfort University before commencing the interviews. Since the research involved human interaction in the form of participants' interviews, the following documents, which can be found in as follows were obtained.

1. A letter from the supervisors to support the research. The letter confirmed that the aim of collecting data was for scientific purposes only, and described how the data was to be collected and held (Appendix 2).
2. Research method and interview protocol (Appendix 3).
3. participation procedures and consent form which explained the research and the requirements and rights of the participants, which was to be signed by both the participants and the researcher to indicate acknowledgement and (Appendix 4)
4. An agreement to participate, shown to the participant prior to the interview (Appendix 5).

The researcher followed the ethical review procedures of De Montfort University (De Montfort University, 2014) in conducting the interviews, and asked the interviewees to read the "Overview and Agreement to Participate in Digital Forensics Research Study" and the letter from my supervisor regarding the research. The interviewees were also asked to sign the consent form.

4.8 Interview Protocol

The researcher developed the interview protocol and tested it during the pilot study. The interview protocol supports the researcher in the process of the data collection. The interview protocol used in the data collection includes the purpose of the interview, general information about the interview, interview guide and checklist, interview questions and a glossary of terms. Further, the interview questions are divided into five main sections (Guidelines and Procedures, Infrastructure, Organisational Policies, Human Resources and Investigation Process) with a total of 29 questions (Appendix 3).

4.9 Summary

In chapter 4 has been discussed the planning and undertaking of the pilot study for the data collection process. The selection of the interviewees and their organisations was justified and ethical issues were addressed. The pilot study protocol has been explained, including the research's objectives, design of the instruments and documentation, the execution of the pilot study, and the lessons learned from it.

The Pilot Study guided the researcher that the data collection tools of Grounded Theory must follow constant comparison and the researcher must take notes of emerging themes during the data collection process and data analysis. The researcher also realized the need to create categories and subcategories during coding. During the data gathering stage, the researcher needs to prepare for the three types of questions used in Grounded Theory: opening questions, intermediate questions, and ending question (Charmaz 2006).

This chapter also explain issues related to the planning and commencement of the research project's data collection process. The selection of interviews was justified in section 3.6 and ethical issues were considered. The interview protocol was explained, including the purpose of the interview, general information about the interview, interview-guide and checklist, examples of interview questions, and glossary of terms.

Chapter Five: Data Analysis

5.1. Introduction to the Application of Grounded Theory Procedures

This chapter explains how the researcher applied Grounded Theory using Straussian techniques to analyse the data collected. It is important to remember that the researcher's application of Straussian Grounded Theory for data analysis presented the interplay between the data and the researcher (Strauss and Corbin 1998, p.13). This complex interplay is not linear, rather creative and systematic (Strauss and Corbin 1998; Strauss and Corbin 1990).

The heart of the Grounded Theory procedure, as described fully below, is the coding of data, which in this research means the interviews (cf. Chapter 4). Before going deeper into the application of the coding procedures into this research, it is appropriate to reconfirm the purpose of the procedures as summarized by Strauss and Corbin in the following simplified form:

1. Build rather than test the theory.
2. Provide researchers with analytic tools for handling masses of raw data.
3. Helps analysts to consider alternative meanings of phenomena.
4. Systematic and creative simultaneously.
5. Identify, develop, and relate the concepts that are the building blocks of Theory (Strauss & Corbin 1998, 13).

This chapter is divided into nine sections. Section 5.2 discusses the initial procedures conducted before and during the data analysis. Section 5.3 explains the flexibility in the coding process. Section 5.4 discusses how the researcher applied strategies for enhancing theoretical sensitivity. Section 5.5 discusses the application of the open coding. Section 5.6 discusses the application of the axial coding process. Section 5.7 discusses the application of the selective coding process. Finally, Section 5.8 discusses the application of the conditional matrix and concludes in 5.9.

5.2 Initial Procedures

It is important first to discuss the preliminary procedures before exploring the application of the coding processes. It is also important to note that the researcher created these preliminary procedures during the pilot study (cf. Section 4.5). The procedure and the results were then carried forward into the data analysis for subsequent interviews. Figure 2 is a picture of the researcher's data analysis process.

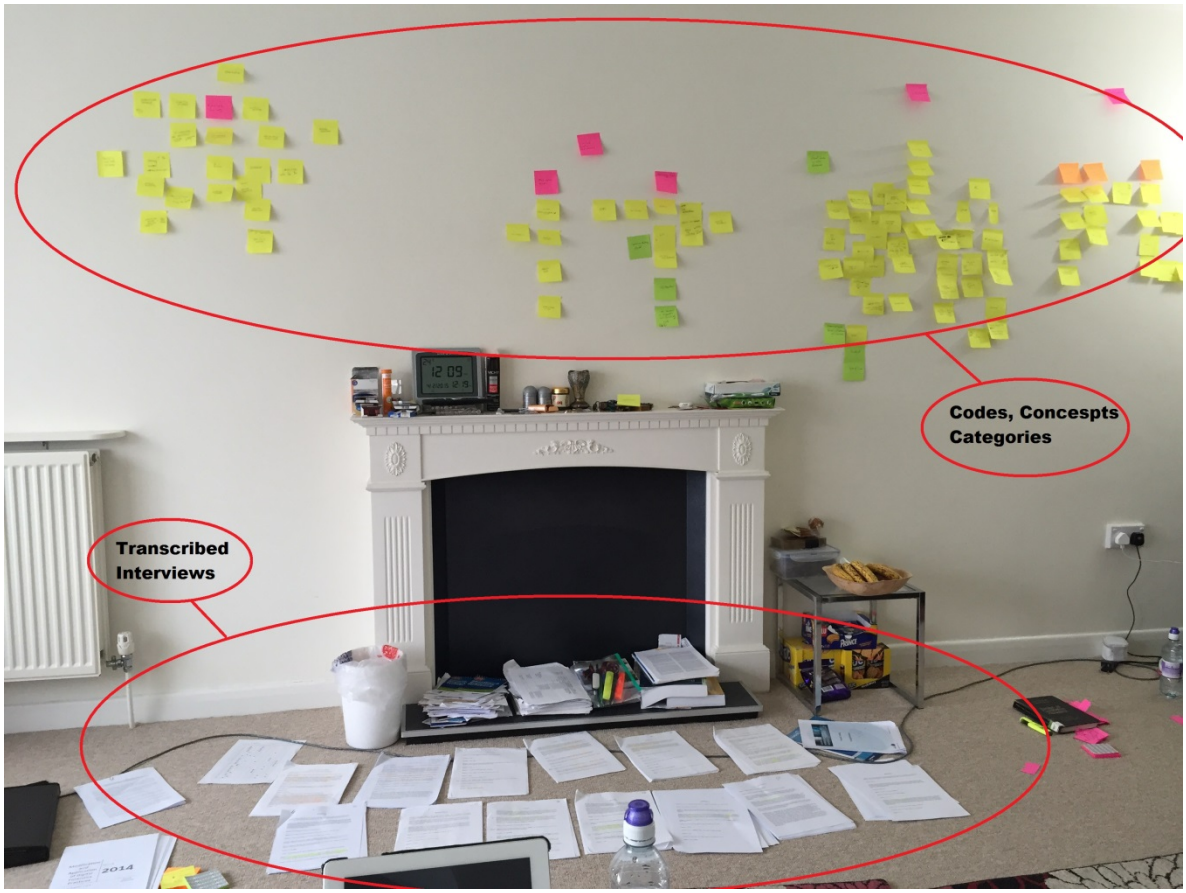


Figure 2 How Researcher conducted Data Analysis in this Research

5.2.1 Transcribing the Interviews

After the Pilot Study, the researcher learned how essential it was to transcribe each interview to enable immediate coding before the next interview. This was important for reaching theoretical saturation (cf. Section 5.3.3), because of the coding procedures under Grounded Theory, and hence the researcher can benefits and increases theoretical

sensitivity from each set of interview data (Strauss & Corbin 1990). The researcher, therefore, aimed at leaving enough time between the interviews for transcribing each interview. The researcher succeeded in doing so in the first six interviews. However, a group of interviews (09MDINTUAE14, 10KSINTUAE14, 11CTINTUAE14, 12CTINTUAE14) were conducted fortuitously and became part of the "fortuitous sampling" (Strauss & Corbin 1990, p.184). These interviews were not transcribed immediately and consecutively but as a group because they were conducted during the Dubai Technology Show (GITEX 2014) held in the Dubai World Trade Centre. Fortunately, theoretical saturation had already been achieved in the data before getting to the "fortuitous sampling" interviews. As discussed below, theoretical saturation was achieved after the fifth interview. (cf. 6.3.3.). The researcher coded each interview and the accompanying interview notes. The researcher took notes during the interviews, to keep track of emerging trends. (cf. Section 4.4).

5.2.2 Assigning Codes to the Interviews

The researcher generally adopted the technique from the Pilot Study (cf. Section 4.5) of assigning "faceted codes" for each interviews with only slight modification. The faceted code was used because they convey more meaningful information and was therefore much easier to use in grounding the data. In the Pilot Study, the faceted code "01BLINTUK13" means interview No.1, Blackstage, Interview, United Kingdom, 2013. Here, the faceted code was slightly modified. Since the researcher did not conduct the follow up interviews, the initial number on the faceted code was changed to reflect the sequence of the interviews. As it turned out, this decision was beneficial as the two interviews had similar codes except for the initial numbers. The use of sequential numbering in the faceted code also allowed the researcher to be more aware to the sequence of the interviews during coding and recoding and when grounding the concepts and categories to the data. The following were the codes assigned to the interviews.

FACETED CODES
01BLINTUK13
02CONINTUAE13
03ALINTUAE14
04AUINTUAE14
05BJINTUK14
06TSINTUK14
07COINTUAE14
08SLINTUAE14
09MDINTUAE14
10KSINTUAE14
11CTINTUAE14
12CTINTUAE14
13NXINTUK14
14ETINTUK14
15RMINTUK14
16WPINTUK14
17PWINTUAE15
18RBINTUAE15
19DMINTUAE15

Table 7 Research Participants codes

5.2.3 Lessons from the Pilot Study

Aside from the preliminary procedural lessons from the Pilot Study, the researcher also improved the Grounded Theory procedures. In the Pilot Study (cf. Section 4.5), the researcher saw the Grounded Theory procedure as linear, doing open coding first, then axial coding second, and then selective coding third, without going back and forth. Analysis of the data in later interviews, however, made it necessary to cross-reference back and to be sensitive to the previous interviews during the coding process. The researcher realized that the coding process was organic and holistic, requiring the researcher to be sensitive to all the coding processes at the same time while remaining open to new concepts found in the data.

5.3 Flexibility in the Coding Process

5.3.1 Interplay between Open and Axial Coding

According to Strauss and Corbin (1998, p.58), "analysis is not a structured, static, or rigid process. Rather, it is a free-flowing and creative one in which analysts move quickly back and forth between types of coding, using analytic techniques and procedure freely and in response to the analytic task before analysts." It is, therefore, significant to understand that when discussing the coding process later in this chapter, the researcher here actually moved back and forth. As stated by Strauss and Corbin (1990, p.98), "though open and axial coding are distinct analytic procedures, when the researcher is actually engaged in the analysis he or she alternates between the two modes."

"For example, the researcher asked the following question in 11CTINTUAE14 at page 9:

> *…how did you become a … digital forensic specialist?*

The participant replied as follows:

> *I had to undergo, of course, trainings. So I did the tools training." (Almarzooqi et al. 2016)*

In this exchange, the open coding caused in recognising the phenomenon of "undergoing training" led to "tool training" concept. The concept of "tool training" was developed and led to the types of "tool training" including "Access Data FTK training", "Guidance Software Encase training", and "XRY training". The dimensions led to the frequency of training (1-3 times) within a certain period (about one year), and how extensive was the training (overview to specialized). Finally concepts were classified as "Types of Training."

Simultaneously the researcher associated the "tool training" concept, using the open coding process with another category called "DF tools" and subcategory known as "Forensic Analysis Software". They arose from concepts, relating to the tools, which were derived from participant's response when asked about tools "FTK", "Encase" and "XRY". This shows a relationship between "DF Tools" and "Types of Training" Categories. Meanwhile, axial coding was occurring while open coding was taking place. This process is called interplay between open coding and axial coding. The researcher had to use the Paradigm Model (See Chapter 5.6.1) to develop further the axial coding further.

"Forensic Training" was also identified by the researcher which also belonged to the category of "Type of Training." One of advantage of this research mythology is the flexibility in interplaying between processes by jumping back and forth from phenomenon to concept to category and between open coding and axial coding to memoing, to naming categories to establishing relationships between them. There was "constant interplay between proposing and checking" (Strauss and Corbin, 1990, p. 111). Important conclusion from this process drawn is that GT is a composite transactional process of data analysis which moves the analysis back and forth leading to many discoveries.

5.3.2 Application of Coding Tables, Diagrams, and Memos

During the coding process, the researcher employed the Grounded Theory techniques of using tables, diagrams, and memos. Tables were used to list the categories, subcategories and concepts. Likewise, tables were used to develop categories, subcategories and concepts to show their properties and dimension. The researcher added to and removed concepts from these tables until the final table developed.

The researcher also used diagrams to see the relationships among concepts and categories. Of course, diagrams were used at the end to create a conditional matrix for the study.

Finally, the researcher used memos to write down thoughts, ideas, analysis, questions, and comparisons. These memos were important in flushing out ideas, in identifying actions and interactions, linking relationships and in becoming creative with theorising and identifying patterns. It was an essential part of the process, because of documentation, which allowed the researcher to reference back to the memos to follow an idea and to ground concepts, categories, and theories.

5.3.3 Theoretical Saturation

"The general rule in grounded theory research is to sample until theoretical saturation of each category is reached" (Strauss and Corbin, 1990, p. 188; Glaser, 1978, pp. 124-126; Glaser and Strauss, 1967, pp. 61-62, 111, 112). Theoretical saturation is reached when "(1) no new or relevant data seems to emerged regarding a category, (2) the category development is dense, and (3) the relationships between categories are well established and validated" (Strauss and Corbin, 1990, p. 188).

The researcher seemed to have reached theoretical saturation after the interview 05BJINTUK14. At this point, there were no new categories emerging. The relationships among the categories were not changing and seemed well established and grounded on the data, and the category development was dense, as there were sufficient subcategories in each category.

5.4 Application of Strategies for Enhancing Theoretical Sensitivity

During the coding processes described below, the researcher applied two strategies for enhancing theoretical sensitivity: (1) "the asking of questions" or questioning, and (2) "the making of comparisons" or constant comparison (Strauss and Corbin 1990, p. 62). These two strategies assisted the process of data to be analysed accurately, precisely, innovatively, and openly (Strauss and Corbin, 1998, p. 73; Strauss and Corbin, 1990, pp.62-63). This

section demonstrated how the researcher applied these two strategies to be presented at the interviews.

5.4.1 Application of Questioning

To open up the data, the researcher used questioning strategies which allowed him to consider potential categories and their properties and dimensions (Strauss and Corbin, 1990, p.77). The fundamental questions, which the researcher utilized as a guide, were the 5W's in addition to 2H, and Who, What, Where, When, and Why in addition to How and How much (Strauss and Corbin, 1990, p.77). Various questions arose naturally as the researcher carried out the analysis the data. The researcher also used Memoing while employing the questioning technique to record the process for referencing and making them more systematic. An example is the following memo:"

MEMO	04AUINTUAE14	11.20.14	QUESTIONING
The subcategory "Preservation" came from and with the concepts "Imaging" and "Duplication." This raises many questions that need to be elaborated and answered either from the data or the literature. Who conducts the preservation? Is it the same person through the entire investigation process that does the preservation, analysis and reporting? There seems to be a step before preservation as well, which is identification. Do the steps have to happen in sequence or can they go back and forth throughout the investigation process. How many copies must be made or preserved? Does it matter? Where is the imaged digital evidence stored? Does this now have a relationship with the tools used in terms of storage? How long after the seizure of the DF evidence must the imaging or duplication take place? Is it right after identification? Is there a rule that waiting too long makes it more likely that the evidence has been altered? What are the other purposes of imaging and duplication? What happens to the duplicated data after the investigation ends? Is there a privacy issue here? Should there be a policy of storage and/or disposal of the imaged data? Who is in charge of this whole process? How can the DF org guarantee that he imaged data has been secured from privacy breaches? So many more question			

Table 8 Memo – Questioning" (Almarzooqi et al. 2016)

5.4.2 Application of Constant Comparison

Grounded theory is frequently referred to as "constant comparative method of analysis" (Strauss and Corbin 1990, p. 62; Glaser and Strauss, 1967, pp. 1-116). Making comparisons is vital to detecting and classifying concepts (Strauss and Corbin, 1990, p. 84). Constant

comparison is, therefore, applied throughout the coding process from open, axial, to selective coding and through each of the data settings. Again, wherever possible, the researcher applied Memoing when using the constant comparison strategy technique to make the process systematic and recorded for later referencing. Here is an example of a memo for constant comparison:"

MEMO 04AUINTUAE14 11.20.14 COMPARISON
In the previous memo, I asked the question: Do these step have to happen in sequence or can they go back and forth throughout the investigation process. It is therefore important to compare the sequences or phases of the investigation process. So comparing the process of preservations with identification. Do both processes take the same time to do? Does one take more time than the other? Why do they take different time? Time is a property with dimensions of hours to months. It would be interesting to compare the time dimensions for each of the processes. Then perhaps to compare the causes of the delay or time challenges. Are they caused by people, tools, process, or policy? Are the skills required for each of the processes the same? There seems to be more skill required in analysis compared to preservation. Is this true or is a specialized skill needed in instances where the evidence to be preserved may be at risk of destruction or corruption. Can the processes be rated in terms of difficulty? The dimension could be from least difficult to most difficult. Does the difficulty related to the tools used, the skills of the people involved or some other intervening cause like third parties or constraints in the investigation?

Table 9 Memo – Comparison" (Almarzooqi et al. 2016)

5.4.3 The Role of Literature and Researcher Experience

The Straussian Approach of Grounded Theory allows the researcher to consult literature before starting the data gathering and their analysis (Strauss and Corbin, 1990). This is one of the distinctions between the Straussian and Glaserian approaches. Literature, therefore, played a role in the data analysis.

First, literature initially guided the researcher and was part of adding theoretical sensitivity to the data. As stated by Strauss and Corbin, "literature can be used to stimulate theoretical sensitivity by providing concepts and relationships that are checked out against actual data" (Strauss and Corbin, 1990, p. 50). The literature helped to frame the research questions that were used for data gathering (cf. Chapter 4). In other words, the literature helped "direct theoretical sampling" (Strauss and Corbin, 1990, p. 52). Also, literature was the source, at

some occasions, for naming the categories, as explained below. (cf. Section 5.5.3.). Literature can also be used as a secondary source of data, to stimulate additional questions, and for supplementary validation (Strauss and Corbin, 1990, p. 52).

Of course, the researcher's experience in the field of DF also added to his theoretical sensitivity. And while the researcher's experience was not used only as a data collector, it was drawn on "for the purpose of sensitizing the researcher to the properties and dimensions in data" (Strauss and Corbin, 1998, p.59).

5.5 Application of Open Coding Procedure

Open coding is the phase of the Straussian Grounded Theory analytical procedure that "pertains specifically to the naming and categorising of phenomena through close examination of data" (Strauss and Corbin 1990, 62). In this research the following steps were taken by the researcher to apply the open coding:

(1) Label the phenomena to become concepts, then put each concept under categories and relate each category and subcategories with each other wherever appropriate.

(2) Develop categories and subcategories by finding their properties and dimensions.

(3) Grounding the concepts, categories and subcategories for the interviews.

5.5.1 Initial Microanalysis Open Coding and Subsequent Coding

Open coding is flexible. "There are several ways of approaching the process of open coding" (Strauss and Corbin, 1990, pp. 72). The researcher is allowed to become interactive with the data per his needs. For example, the researcher may conduct the analysis line by line, sentence by sentence, paragraph by paragraph and complete document analysis (Strauss and Corbin, 1990, pp.72-73).

The researcher, therefore, started the open coding process with a line-by-line analysis, or microanalysis (Strauss and Corbin, 1998, p.57) for the first (03ALINTUAE14) and second interview (04AUINTUAE14). Later the researcher applied the analysis both, sentence by sentence and paragraph by paragraph analysis.

5.5.2 Labelling Phenomena or Concepts from the Data

According to Strauss and Corbin (1990, p. 63), the first step in the data analysis is its conceptualisation, which is consist of finding the "central idea, event, happening and incident" in the data which is called a phenomenon. This describes an action or interaction or a set of actions and naming it (Strauss and Corbin, 1990, p. 96). After conducting detailed analysis of the first two interviews, the researcher recognised the following:

PHENOMENA: ACTIONS DESCRIBED BY PARTICIPANTS	**CONCEPTS**
Handle cases	Investigation
Must finish a case in limited time	Deadline
Must follow an investigation process	Investigation process
Must stay within scope of investigation, cannot investigate everything	Scope of investigation
There is a documented process to follow, conducts DF investigation based on experience	Documented process and procedures
Look at a reference point, no absolute standard exist	Multiple standards
Follow usually, follow experience, experience dictates what to do	Best practices
Adopting international standard, made our own standard, inherited from interpretation, follow ISO standard, meeting the standards, we use our own book as standard	Standards
A guideline relates to it, a guideline does not exist, not required to follow guideline	Guideline
Vendors provide training	Vendors
Having a process in place, follows a process	Process
Follows a workflow	Workflow
Pressure felt by DF investigators	Time constraint
Must follow the DF framework	DF investigation framework

Follows ethics as a guideline since no standard	Ethics
Work and data must be verified	Verification
Work and data must be validated	Validation
DF companies sell experience and services	Organization's scale (size)
Data must be copied and duplicated	Duplication
Data must be imaged	Imaging
Data must be preserved	Preservation
To recover deleted, lost or damaged data	Recovery of Evidence
DF professionals must follow procedures	Procedures
To get evidence admitted in court	Evidence admissibility
To manage evidence	Chain of custody
To maintain a documented trail	Audit trail
2: Scenarios at crime scene:	
Must use forms	Forms
Customizes physical layout of lab	Infrastructure
3: DF industry	
Tech changes all the time, must keep up with new technologies	Evolving technology
4: Multi discipline field	
People are the key to success (9p4)	Quality of people
Consider the type of DF entity	Private
Consider the type of DF entity, policing differs from enterprise	Law enforcement
A DF investigator must think like a criminal, ability to give court testimony	DF Investigator Characteristic

Consider the type of DF entity	Public
Built a lab for a university	Academic purpose
Built an education lab	Education lab
To hold someone responsible for the lab actions	Accountability
To select proper tools, to use proper tools	DF tools
To manage and maintain the DF lab, to manage cases that come in, update operations manual, approved change management procedures, small team is no hassle to manage	Lab Management
There is a management hierarchy, work is assigned by management, how work is assigned	Organizational hierarchy
Lab uses different software	Software
Lab uses hardware	Hardware
5: Minimum factors	
To reuse components	DF lab equipment
Type of crime or services determines capacity of organisation	Type of crime
To block access or changing data	Write blocking
To report data	Data Reporting
To acquire or find data	Data Acquisition
To conduct crime scene investigation	Mobile (on site) forensic
To conduct crime scene investigation	Mobile forensic work station
To set up capability and respond to different scenarios, individual capacity according to department	Capacity of lab
To have proper equipment	Laptop and desktop
To have proper tools and equipment	Accessories

Commercial tools do more than one thing	Multipurpose forensic analysis tool
Service offered	Malware analysis
Not used for investigation, not used for storage, used in limited scope	Cloud
To make job easier, easy to use tool, use the right tool for the right job	Tool selection
6: Not depending on one tool for investigation	
Services offered determines scope of lab	Scope of lab investigation
Use commercial tools	Commercial tools
To determine type of work lab performs	Purpose of lab
To conduct mobile phone forensic	Mobile phone forensic software
Selects tool based on function	Functionality
DF investigators analyses data	Analysis
Commercial tools do multiple tasks	Multi functionality tools
Restrained by cost and budget	Cost and budget
Determine and set policy on who has access to lab	Authorized access
Accreditation bodies exist	Lab accreditation
Consider whether to get accreditation	Reason for accreditation
Accreditation to set quality standard, ISO shows there is quality standard	Quality assurance
To build a lab	Building a DF lab
Identify the budget range	Budget
Buying equipment for lab is biggest challenge	Equipment purchasing

Determine what the lab needs	Requirements for DF lab
Determine the purpose of the lab	Professional training lab
Features of a lab	Internet access
Research is important to keep up to date or ahead, to forecast crime	R&D
Ability to provide DF services, ability to fight crime	DF Capability
Identify type of capability , capability rests with people	Capacity of DF organization
Must set policies	Policies
Guideline for managing activities	ACPO
Follows ISO-17025 (for DF labs), follows ISO-17037 (handling digital evidence), ASCLD, ISO-9001 (general quality), not necessary to follow ISO	ISO
Maintain a log of activities	Log or record of access
To control who gets in and out of lab	Access/control of lab
Staff must train	Training and development
Staff must focus or specialize on one type of DF investigation	Specialization of DF staff
To give employees orientation upon hiring, to teach employees about the policies	Employee orientation
DF investigator should have/not have degree, experience, knowledge, skill in related field	DF investigator qualification
Type of degree is unclear, degree in related field is preferable	Education and training
Difficult to find DF practitioner	Limited DF practitioner
Certification is not necessary but good to have	Certification

Has IT management experience, has security experience, experience based approach	Experience
7: DF investigator prior background	
Type of experience to have	Industry experience
Type of experience to have	Theory v practical experience
8: DF education	
Before becoming DF investigator	DF Investigator prior background
To train based in what is needed, to keep with emerging technologies	Need based training
Types of training offered	Procedure based training
Types of training offered	Tool based training
9: Open source intelligence	
To acquire qualification for DF, to acquire knowledge of DF	Academic degree
Follows a model for determining capability	Capability Maturity Model

Table 10 Concepts and Phenomena's

5.5.3 Creating and Naming Categories and Subcategories

After identifying the set of phenomena and concepts it is divided into categories and subcategories, this is conceptual categorisation (Strauss and Corbin, 1990, p.65). “Categories have conceptual power because they are able to pull together, around them, other groups of concepts and subcategories” (Strauss and Corbin, 1990, p. 65).

The researcher then, following the Straussian approach of Grounded Theory, arranged the concepts generated by grouping them under categories. The categories naturally evolved and sometimes they were renamed, similarly with concepts as they were re-categorised as new concepts produced and developed.

The names of the categories are created by the researcher, but at times the names were taken from the literature (Strauss and Corbin, 1990, p. 68), or from the words of the interview participants themselves, called "in vivo codes" (Strauss and Corbin, 1990, p. 69). For example, the category "*Small Scale Devices*" was taken from the Mousa Al Falayleh's article "Building a Digital Forensics Laboratory for an Educational Institute," an article which discusses in detail the minimum software and hardware requirements of building a DF laboratory for educational purposes. The phrase "*Small Scale Devices*" did not appear in the data but covered many concepts described by the participants like "*Oxygen Forensic Suite*" (15RMINTUK14), "*Faraday Bag*" (07COINTUAE14), etc.

Alternatively, the names of certain categories came directly from the participant like the "Operational Manual" which came from interview 03ALINTUAE14, where the participant stated as follows:

> "*You have to keep on updating your operational manuals…so the management of lab comes in this way…*" (03ALINTUAE14, p.3)
>
> "*So I would rather make a module or an operational manual for an Android device*" (03ALINTUAE14, p.3)
>
> "*That covers from operational manual to policies and procedures to work instructions*" (03ALINTUAE14, p.18)

It was often the case when a participant used a word or phrase that came from the literature. An example is the phrase *"Capability Maturity Model"*, which was not only used by the participant in 03ALINTUAE14 but also appears in the literature.

In most instances, the categories were named and created by the researcher to cover multiple phenomena that arose from the data and from the open coding process. An example of how a group of concepts was categorised is the "DF Investigation Process." The category came to be after the concepts of "*preservation*", "*imaging*", "*duplication*", "*analysis*", and "*reporting*" were first identified in the following response by a participant, which was found in the interview with faceted code 04AUINTUAE14:

> *"…something I really took care of is … with the digital forensics. There is a framework which is very famous framework to do the digital forensic investigation which is the preservation and then do imaging, duplication, and then the analysis and end up with the reporting, right?"* (04AUINTUAE14, p. 2).

Ultimately, the researcher named the category "DF Investigation Process" because it seemed to pull together concepts that name a set of actions and interactions that make up the investigation process. In other words, the participants were describing the steps in the investigation process. After further Memoing and analysis, the researcher made the concepts "preservation", "analysis" and "reporting" as subcategories of the category "DF Investigation Process" because, what became subcategory "preservation", for example, covered the concepts of "imaging" and "duplication". These were actions and interactions that a DF investigator engaged in for the purpose of preserving the evidence.

5.5.4 Developing Categories and Subcategories with Properties and Dimensions

Categories and subcategories were developed according to their properties and dimensions, "properties are the characteristics or attributes of a category, and that dimensions represent locations of a property along a continuum" (Strauss and Corbin, 1990, p. 72).

One way of expanding categories is to identify any possible properties and dimensions for each category identified. The properties are features or attributes of the categories whereas the dimensions are settings of a property along a continuum. Identifying the dimensions of categories in DF often was challenging but several of these categories were easily given the dimensions. Also, identifying the dimensions and properties of a category in DF made the

relationship of the property, dimension, and the category viewable. In this sense, axial coding occurred simultaneously during the open coding process, which is unavoidable (Strauss & Corbin, 1990). Generally, expanding the categories with properties and dimensions lead to a richer set of coding that made the theoretical memoing much richer as well. The researcher then was able to discuss aspects of the categories that would have been largely ignored without engaging in these more detailed steps in the Grounded Theory process.

Table 11 presents the category" **Investigation Process**" which has been developed by the researcher using properties and dimensions:

CATEGORIES	**PROPERTIES**	**DIMENSIONS**
Investigation Process	Human Factor	No. of investigators
		Level of the investigator's skill
	Challenges	Time
		No enough resources
		Size, Volume
	Financial Budget	Amount of money
	Case Load	No. of Cases
	Time: Length of Process	Time frame
	Size of Data	Volume, size
	Types of Cases	Criminal
		Financial
		Research based

Table 11 Developing Category

5.5.5 Grounding to the Data

After identifying concepts and categories by the researcher in the coding procedure, he used the faceted code of each interview and the page number to ground the data. This process concurrently made it easier to refer to the interviews while writing Memos. Grounding the data this way allowed finding weak arguments in the research that required additional data.

5.6 Application of Axial Coding Procedure

Axial coding is the process of establishing connections between categories and subcategories by placing the data in new ways to achieve this connection (Strauss and Corbin, 1990, pp. 96-97). Relating categories and subcategories can be achieved in three steps:

1- Apply Axial coding using paradigm model
2- Develop the categories using the paradigm model
3- Identify the properties and dimensions of each category and subcategory.

Next section demonstrates the application of axial coding the in the data.

5.6.1 The Paradigm Model

The paradigm model in figure 3 shows the process of building relationship between subcategories and categories in 6 stages as shown below (Strauss and Corbin, 1990, p. 99).

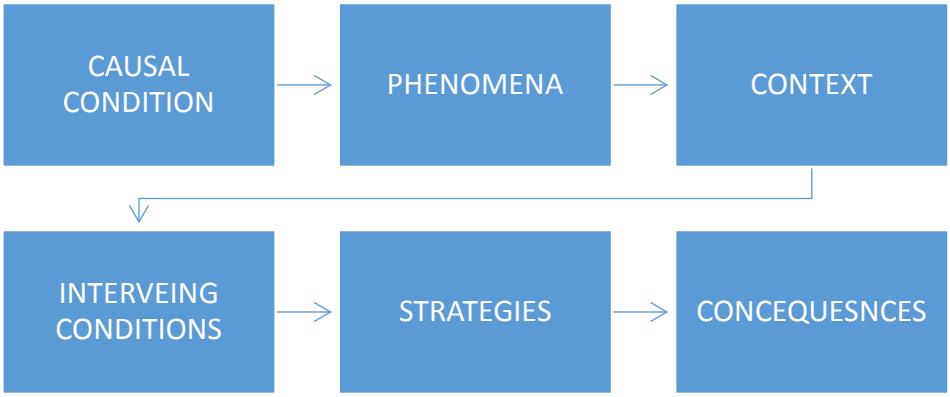


Figure 3 the Paradigm Model

Strauss and Corbin (1990, p.99) emphasized the use of the paradigm model in GT and failure to use it will lead to "lack of density and precision" (Strauss and Corbin, 1990, p.99) in the analysis.

The researcher used the paradigm model to connect subcategories and categories by building their relationship. Table 12 presents an example of using paradigm model in the research.

Causal Condition	**Phenomena**	**Context**	**Intervening Conditions**	**Strategies**	**Consequences**
Crime	Investigation	Presence or potential presence of digital or evidence	Destruction of Digital Evidence	DF Investigation Framework	Finding of Evidence
Digital device at crime scene	Type of DF investigation: computer, mobile, network, cloud, internet		Challenges to Investigation	Identification	Not finding evidence

Table 12 Example of using Paradigm Model

5.6.2 Developing Relationships

The axial coding is complicated process especially connecting and developing categories (Strauss and Corbin, 1990, p.107). The process requires the concurrent act of,

1-Relating subcategories to categories

2-Verifying hypothesis with actual data

3- Identifying properties and dimensions

4-Identifying variations in the phenomena

And this can be achieved through constant comparison of categories and subcategories (Strauss and Corbin, 1990, p. 107). The categories and subcategories were developed after

collecting and analysing the data using procedures explained in 5.2 and 5.3. The transcribed interviews were micro analysed to extract codes and concepts and then grouped them together as shown in figure 2. This process developed in categories and subcategories is presented in Table 14:

CATEGORIES	**SUBCATOEGORIES**
Investigation Process	Purpose of Investigation
	Scope of investigation
	Identification
	Preservation
	Analysis
	Reporting
	ACPO Principles
Evidence Admissibility	Data Verification and Validation
	Chain of custody
	Qualification of Investigator
	Expert Testimony
	Vulnerable to Legal Challenge
	Authentication
Investigation Procedure	Documentation
	Standard (ASCLD)
	Pre-Investigation
	Case Management
	Post Investigation
Stakeholders	Private

	Public
Tools	Tool selection
	Forensic Analysis Software
	Standard tool
	Hardware
	Software/Hardware
	Peripherals or Accessories
	Small Scale Devices
Virtual Environment	Cloud
	Virtual DF Labs
Building a DF Facility	Process
	Facility Requirements
	Financial
	Functionality and Purpose
Facility Building and Management Standards	Standards
	Best practices
	Guidelines
	Lab accreditation
	Ad Hoc
	Key Success Factors
Organizational Policies	Information Security Policy
	Physical Security Policy
	Tech Use Policy

	Maintenance Policy
	Confidentiality & Non-Disclosure
	Evidence Storage Policy
	Conflict of Interest
	Operational Manual
	Policy as Capability
	No Policy
	Ethics Policy
	From Standards/Accreditation
Knowledge/Background	IT
	Security
	Law
	General Forensic
	Specialization of DF staff
Education	Type of Discipline
	Quality of Degree
	Necessity
Experience	Industry experience
	Experience Means
	Length of Experience
Training and Development	Types of Training
	Training as Qualification
	Development

	Certification
	Self-Education
	Necessity
Organizational hierarchy	Management
	Technical
	Administrative
	Size of Organization
	Type of Organization
Investigator Trait	Investigative
	Communicative
	Technical
	Analytical
	Motivated
	Creative
	Aptitude
	Security Clearance
	Quality of people
Capability	Definition
	Standards and Guidelines
	Capability Maturity Model
	Gap Analysis
	Benchmarking
	Minimum Factors

	Policy as Capability
	DF Readiness Check
	Individualized

Table 13 Categories and Sub Categories

5.6.3 Grounding to the Data

After identifying the concepts and categories by the researcher in the coding procedure, he used the faceted code of each interview and the page number to ground the data of subcategories and categories.

5.7 Application of Selective Coding

The final step in data analysis is selective coding, which is the "process of selecting the core categories, systematically relating it to other categories, validating those relationships, and filling in categories that need further refinement and development" (Strauss and Corbin, 1990, p. 116). The process of selective coding is relatively like axial coding, because it requires recognising relationships; however it is "done at a higher and more abstract level of analysis" (Strass and Corbin, 1990, p. 117). In this section the researcher demonstrates how he applied selective coding, in section (5.7.1) explain the story line, in section (5.7.2) relate categories and subcategories to the core categories, in section (5.7.3) relate categories at the dimensional level, and in in section (5.7.4) validate the relationships by grounding the theory to the data (Strass and Corbin, 1990, p. 117-118).

5.7.1 The Story Line

Before trying to identify the story line, Strauss and Corbin (1990, p.119) suggest that the researcher should ask about what it is most striking that stand out in this research about the core categories and the subsidiary categories. In a memo on the story line":

MEMO 02/02/15 STORY LINE
What is most striking here are the different ways that people think about the concept of capability in the context of DF lab building and management. Some understand capability in terms of the DF tools available in the organisation; others understand capability in terms of the people or the human resources, while others understand capability as having both the DF Tools and the human resources. Others still view capability in terms of their ability to act and/or interact in the context of the challenges they face during the DF investigation process. While many recognise policy as necessary in the DFO, it is not readily identified as a component of capability.

Table 14 Story Line Memo"

5.7.2 Identifying Patterns and Core Categories

The researcher then recognised patterns in the categories and subcategories. He then used paradigm model, diagrams and memos to identify patterns and the fact that categories and subcategories are related and helpful to specify their dimensions. Thus, four core categories emerged from the categories: (1) Investigation, (2) Infrastructure, (3) People, and (4) Policy (Almarzooqi and Jones, 2016). The four core categories of capability have been defined in the data and the literature.

5.7.3 Relating the Categories at the Dimensional Level

The researcher then related the core categories to their dimensional level. One detailed example in core category "investigation" which is consist of three categories "investigation process", "evidence admissibility", and "investigation procedure"; when applying selective coding, the data show that they are related to their precise dimensions. "Investigation process" category is presented in table 15 and shows the properties and dimensions of the "investigation process" that can be related.

Investigation Processes	
PROPERTIES	**DIMENSIONS**
Human Factor	No. of investigators: 1-5
	No. of specialization needed
	Investigator skill level
Challenges	Time: limited to unlimited
	Resources: limited to unlimited
	Data Volume: low to high
	Trust: low to high
Results	quantity of data identified: low to high

Table 15 Example of Relating Categories

The properties and dimensions found in the category of "investigation process" are linked to the core category of "Investigation". For example, the number of investigators is an unavoidable factor because DFOs stand on them and their number in one way of determining their capability. Therefore the researcher identifies the need for a ratio to determine the number of investigators and number of cases assigned to them for a given period of time.

The above statement also related to additional dimension in the same core category the property "Challenges", which means that investigation process face challenges such as a dimension of "time constraint" which can be measured by amount of time available. This dimension comes under the property "Challenges" and related to "number of investigator" in another property "Human Factor". Therefore dimensions mentioned were linked and bound to the core category "Investigation".

In addition to that, a relation between "Number of investigators" to the core category "People" has been identified by the researcher, where "number of investigators" became a

dimension in that core category. Similarly “number of investigators” as a dimension was also appropriate in core category, “Infrastructure”, because “Building a DF Facility” and the subcategory “Facility Requirements” steered to “people” or “staffing” concepts. To be more specific, “number of investigators” as a dimension was needed through core categories in 1) Determining staffing needs (core category “People”), 2)Detecting preliminary staffing needs in “Building a DF Facility” (core category “Infrastructure”) both affected “Challenges” based on “Human Factors” according to the ability of the investigator. This type of relation between category and other core categories supported the researcher to distinguish between the similarities and differences of the role of the dimension in the individual core categories. Indeed, several relationships and linkages rose from the dimension of “number of investigators”.

The above example shows the importance of relating the core categories and categories at the dimensional level which is crucial phase in the selective coding process because it makes the theory development more specific by relating precise measures in the dimension to the higher level categories and through higher level categories.

5.7.4 Grounding the Theory to the Data

The final step in the selective coding process is to validate the relationships among various categories and connecting them to the data. This validation process occurs mainly at the conceptual and dimensional level, therefore emphasizing the need to relate higher level categories to the dimensional level.

The coding process forces the researcher to ground the data in open and axial coding so it can be used at the selective coding process. The previously grounding of data was at the detailed level and therefore it becomes easier to ground at abstract phase of coding, when grounding was already existed.

For example, the dimension “number of investigators” was grounded by interviews which were also grounded during open, axial, and selective coding. For example, the need for having a number of investigators was connected to the following interview:

Q: " *how do you define an organisation to be digital forensic capable?*"

A: "*…they should have enough capabilities in term of human resources people have enough experience,*" (07COINTUAE14, p. 4)." (Almarzooqi et. al 2016)

The participant in the above interview used the term "enough" for human resources that can be measured by number and identified as a quantity. On the other hand, the researcher connected the "number of investigators" to "skill level" of the investigator which comes under the category "Quality of Investigator"; this was related and looked at in the core categories "Infrastructure", "Investigation", and "People". In other words, grounding the theory also led back to the coding process, showing how grounded theory can interplay between inductive and deductive analysis.

5.8 Application of the Conditional Matrix

Strauss and Corbin defined a conditional matrix as "an analytic aid, a diagram, useful for considering the wide range of conditions and consequences related to the phenomenon under study, enabling the analyst to both distinguish and link levels of conditions and consequences" (Strauss and Corbin, 1990, p. 158). It is this process of integrating the small details to the procedures, operational logic, categories, and core categories that are "the hallmark of grounded theory studies (Strauss and Corbin, 1990, p. 159).

Here, the researcher applied the conditional matrix by creating diagrams throughout the coding process, and then combining these diagrams into a final matrix that demonstrates the relationships and action/interactions among the small detailed parts to the larger categorical concepts. Importantly, the matrix took into consideration the action and interaction processes that occur at the individualized level to the organizational, national, and international levels (Strauss and Corbin, 1990, p. 162-163). Taking these multiple organisational layers into account through the conditional matrix added a richer layer of analysis to the study. The conditional matrix diagram is discussed in the next chapter in more detail.

5.9 Conclusion

This chapter explains how the researcher applied the data analysis methodology of Grounded Theory, stressing the non-linear processes of coding through examples of the dynamic interplay among open, axial and selective coding. The systematic application of the coding processes by the researcher is what makes the methodology Straussian in its approach to Grounded Theory. The application of this methodology resulted in a set of findings about the data that is discussed in the next chapter.

Chapter Six: Findings on the Outcomes and Relationships of Core Categories

6.1 Introduction

The chapter discusses the outcomes and relationships among the data that the researcher identified in doing the data analysis (cf. Chapter 5). Section 6.2 discusses the outcomes that the researcher identified from the coding processes. Section 6.3 discusses the relationships among the core categories with the aim of paving the way for a theoretical discussion in the next chapter.

As stated by Strauss and Corbin, "the purpose of grounded theory methodology is to develop theory and not to merely describe phenomenon" (1990, p.167). While the previous section explained the process of data analysis using Straussian Grounded Theory and its application to the research at hand (cf. Section 5.2), this section discusses what the researcher identified as outcomes and relationships from the numerous and dynamic micro and macro coding processes that occurred during the analysis. The first part is discussing the different core categories, categories, and subcategories that the researcher has identified, and then the second part focusing on the relationships between the categories and core categories.

6.2 Identified Categories and Subcategories of Digital Forensics Capability

This section discusses the outcomes from the coding processes, incorporating all three types of coding into one. During the coding process, the researcher added to and deleted from the table used during open, axial, and selective coding. The final result of the categories and subcategories identified from the coding process is discussed in this section. Before discussing the core categories, the researcher first discusses the categories and subcategories identified.

The researcher identified a number of categories and subcategories during open, axial and selective coding. There were instances when the researcher had to change the names of these categories or subcategories to reflect instances when concepts were upgraded to

subcategories, and subcategories to categories and vice versa. The full list of these categories and subcategories were already shown in Section (5.6.2.). The following, therefore, is the discussion or explanation of each category and their respective subcategories.

6.2.1 Investigation Process

The category of "Investigation Process" is perhaps one of the most important categories and one which surfaced in every interview. The centrality of the investigation process to DFC lies in its function: it is at the heart of the actions and interactions of DF professionals. In the paradigm model, the investigation process encompasses the action/interaction strategies, simply because this is where the action happens. For this reason, the initial focus in DF research has been to create frameworks or models for explaining the investigation process, which is discussed in more detail in the next chapter (cf. Chapter 7).

"Investigation Process" became a category in this research because of the data, and the concepts and phenomena identified from the interviews of participants. It is, therefore, important to explain the subcategories of "Investigation Process" and to explain the categories and subcategories in a way that is rooted in the interviews. The subcategories that were identified from the data were: preservation, identification, analysis, and reporting.

6.2.1.1 Preservation

The subcategory "preservation" was referred to in the interviews through the phenomenon of "imaging" and "duplication", both of which became concepts under the "preservation" subcategory. In the interview 07COINTUAE14, the question asked was:

> *"…Can you just briefly go through one of these documented process…"* (07COINTUAE14, p.14).

The participant, in his response, mentioned the following as part of explaining the process of investigating a mobile phone:

> "*I should preserve it in a faraday bag that will disconnect all network communications.*" (07COINTUAE14, p.14).

Another participant discussed the concept of preservation in terms of the basic tools used and the basic capability of a digital forensic laboratory. In interview 08SLINTUAE14, the participant was asked the following question:

> *"…what are commonly used tools in digital forensic labs now, currently?"* (08SLINTUAE14, p.6)

The participants replied as follows:

> *"So, main component is having a write blocker and duplicate them. That's your basic requirement to do any forensic capability, okay?"* (08SLINTUAE14, p.6)

In other words, the ability to preserve digital evidence - the subcategory "preservation", through the phenomenon "imaging" and "duplication", is closely linked to the tools used, as the tools enabled the preservation of data.

6.2.1.2 Identification

In a question about the investigation process, the subcategory "identification" was referred to in interviews 13NXINTUK14 and 08SLINTUAE14:

> *"…the end of the day there's several important parts to an investigation,* one *of them identification"* (13NXINTUK14, p. 12).

> *"So, the main issues in forensics is acquisition. It takes a long time especially if it's a large data sets…"* (08SLINTUAE14, p.22).

6.2.1.3 Analysis

The participants in interview 08SLINTUAE14 discussed the subcategory of "analysis" as part of the investigation process.

> *"It takes another day also to analyse the hard drive. That's even before you start investigating. So once you acquire whatever tool you're using, we'll need to do*

analysis...generate metadata so you can search effectively."(08SLINTUAE14, p.22)

6.2.1.4 Reporting

When asked about potential for improvement (13NXINTUK14, p.11), the participant's response went directly to the importance of reporting in the investigation process, and its relationship with an investigator's ability to communicate.

> *"I do think reporting as well and requires a lot more work …there's several important parts to an investigation, one of them identification, and seizure is obviously another. And then how you articulate the results. If you can't communicate the results in an effective manner, sometimes that key piece of evidence is not understood and missed."*(13NXINTUK14, p.12)

Effective communication, therefore, one of the key characteristics of an investigator under the "Investigator Characteristic" category plays an important part of the investigation process.

The four subcategories: preservations, identification, analysis and reporting are the key phases of the investigation process. While the investigation process may be broken down to further steps, as can been seen in the frameworks proposed in the literature (cf. Chapter 7 Discussion), the researcher found that participants broke down the process into these four phases. The participants discussed these phases within the context of the investigation process as action/interaction strategies for achieving the aims of a DF investigation.

6.2.2 Investigation Procedure

While the category "Investigation Process" covers the phases in the investigation, the category "Investigation Procedures" deals with the phenomena before during and after and surrounding the investigation process. In other words, concepts under this category affect the entire investigation process. The researcher grouped the concepts that arose relating to

the category “investigation procedure” into five subcategories: “documentation”, “standard”, “scope”, “pre-investigation”, and “case management”.

6.2.2.1 Documentation

The subcategory “documentation” groups concepts and phenomena that deal with the documentation of processes in the DFO. The participant was asked the following question:

> *“Do you guys have a documented process for investigation?”* (05BJINTUK14p24)

While the researcher asked about the documented process relating to investigation, participants often responded with a documented process that went beyond the investigation process. Most participants stated that they did have a documented process, as the following examples demonstrate:

> *“Yes. Yeah.” (*11CTINTUAE14p12*)*

> *“Of course, must we. All procedures and during the investigation must be documented.” (*07COINTUAE14p16*)*

> *“I certainly do. …Under operating procedures for investigations that we also know.”* (09MDINTUAE14p14*)*

> *“Certainly in the past, we had a documented process of the steps to follow…”* (13NXINTUK14p10-11)

> *“We did when we finished. We didn’t when we started but we did when we finished.” (*15RMINTUK14p41)

Nevertheless, two participants stated that they did not have a documented process, but instead followed a process based on experience:

> *“No, not really. It depends on the case. You have to make a judgment.”* (05BJINTUK14p24)

*"No, no, no. For us we, we don't have a set of templates for that." (*08SLINTUAE14p19*)*

That two participants did not have a documented process shows the lack of an industry standard on a most basic procedural requirement for a forensic lab. As one participant explained, the purpose of a documented process is to ensure the reliability and verifiability of the investigation process:

*" …documented procedures that need to be followed for each of them so you can repeat the steps and anybody else can actually verify the report." (*09MDINTUAE14p3)

*A: "Yes we have a process that comes….General scenario. That's tackles about the handling of the incident and handling of, for example, hard disk, carving hard disk wiping, hard disk…but definitely it cannot cover all of the cases because as I've said, there we have some unique cases that makes both of them." (*12CTINTUAE14p10*)*

A: "Yes. Actually we have a process which is also incorporate training to have to start by handling the evidence. So if we were to do suspecting…which is very important by the way because it might be, it will be used later on as a repetitive lead, etcetera…during the investigation and during ah…the report for example that we are following the, we are prosecuting the criminals. And of course you need to start with the process from the beginning and the end of the investigation and especially in the beginning because it is very critical to ah…collect the evidences as they are and protect their integrity." 10KSINTUAE14p12*)*

A*: "Okay. So we have two things that we do. We have a case management system like you see hits…so from…it's a right…you've got to six server. Now you got to*

*open her up, right? And you've got to photograph it…have you photographed it. Have you done this, have you done that. Right, what type of job is that. I'm going to use Encase on ahm…I'm going to use….have you done, you know, have you done, have you write blocked her…you know, back to basics that is…it just sort of gives you hints. …And we've got also on top of that we've got ISO, so ahm…we try and ahm…write up, you know, step by step how to use a particular software, how to use a particular data. So yeah, we have quite a bit of both." (*16WPINTUK14p20-21*)*

A: "Yes. There is…there is a process that doesn't define and I'll be happy to share it with you, but it doesn't define how to investigate. It defines the…it doesn't define the methods in the investigation, it defines the stages, if you like, and the processes that you need to consider." (14ETINTUK14p32)

*A: "Documented procedures. That that's exactly it. It's about documented procedures, showing those documented procedures work." (*14ETINTUK14p19)

*A: "It's based on a standard. The standard we follow has all the steps, beginning from one we receive the evidence up to the labelling, up to the storage, up to what investigation has to be done until we get the final reports published." (*11CTINTUAE14p12*)*

6.2.2.2 Standard

The subcategory "Standard" groups concepts and phenomena that deal with following standards for processes in the DFO. The participant was asked the following question:

*A; "So we follow the standards and the analysts has to go through all the necessary forms indeed." (*11CTINTUAE14p12)

*A: "…we must be also precise because we need to follow the quality standard with us even though we have a workload." (*12CTINTUAE14p3)

6.2.2.3 Scope

A participant discussed the "scope of the investigation" as an important consideration in the investigation procedure. The participant touched on the investigation as needing to have a scope, and making the identification of that scope as part of the procedure. In interview 15RMINTUK14, the participant stated the following:

> "*So we have actually had to say, 'well, you going to have to fill in some forms here' because we need to know, when was it seized, this person in custody…what is it that you want us to get from that examination? And it's no good just saying, here we want everything, which is what they used to say, we want everything. Well, you can't do it. Everything is just huge amount of data.*" (15RMINTUK14, p.3).

> *A: "So the first step is to identify is the nature of the forensic analysis that's going to be taken. So first, in order to design processes and procedures, the first step is to identify what work you're likely to undertake. …The type of forensic work that you're going to do.*" (14ETINTUK14p4)

> *Q: "So, the exact scope of your work?"*
> *A: "Yes, so that…you can focus…The amount of data there are, even on a smartphone today, is vast. And really you must have some focus. Otherwise, when do you stop? And my criteria for stopping was as soon as you've had enough evidence to prove the case." (*15RMINTUK14p3)

6.2.2.4 Pre-Investigation

The participant answering question regarding any procedure prior to investigation:

> *A: "And then we do something called primary check. So this primary check is basically to identify what is the status of the evidence right now and what is the most I can get according to this status."* (07COINTUAE14p17)

6.2.2.5 Case Management

A participant discussed the job assignment mechanism and handling responsibility as an important consideration in the investigation procedure. The participants touched on the skills, workload and best person to handle a certain task.

> *Q: "How do you guys exercise authority on them? How do you assign jobs?"* (11CTINTUAE14p9)
>
> *A: "…tasks are assigned based on round random, so we have a ticketing system that comes into the lab and they're handled by whoever is available."* (11CTINTUAE14p9)
> *A: "I go through their workload. I understand where they are with cases and I can work out what their abilities to take some more cases or not. And for me, I find it easier to have a conversation with the high tech officer, try of sort give and take, rather than dictate…"*(16WPINTUK14p14)
>
> *A: "It's…the assignment from the beginning, the assignment go to the best person who can handle this case."* (07COINTUAE14p13)
>
> *A: "So, obviously, skills is a primary decision-maker, so to say. If one person is more skilled than the other, the person most suited for this job at hand, this is the one that will be doing the job, and, of course, then availability is as a matter…" (*09MDINTUAE14p10)

6.2.3 Evidence Admissibility

The data showed that participants were widely concerned about the admissibility of DF evidence in court and making sure the process of DF investigation took into account the issue of "evidence admissibility," which then became a category. In other words, whenever

participants discussed the investigation process, they also discussed concepts related to "evidence admissibility", which was labelled a category consisting of "concepts" that grouped together into the following subcategories: "data verification and validation", "chain of custody", "legal challenge", "qualification", and "pressures".

6.2.3.1 Data Verification and Validation

The subcategory of "data verification and validation" appeared in two related concepts whenever participants discussed the DF investigation process: the use of multiple tools to verify and validate data and the use of a peer review system. Regarding the use of multiple tools three participants stated as follows:

> "*…there is some rules that you should have or some rules that you should use like using multiple tools for using the same purpose*" (07COINTUAE14, p.1).

> "*…if I had one tool that was able to do X, I need to get another tool that could do X as well.*" (13NXINTUK14, p.2)

> *"So for me it's flexibility and the ability to compare results between the tools…Data verification."* (14ETINTUK14, p.16).

The three participants above, in essence, expressed the concept of using more than one tool so that a secondary or even tertiary tool could be used to verify the findings of the first tool. This concept has two implications for the research. First, the investigation process is closely tied to the selection and decision on what tools to use and the number of tools to use. In other words, the investigation process itself dictates a minimum requirement for the number of tools a laboratory must have at least two for purposes of verification. Second, the investigation process as a category relates directly to a separate core category of "Infrastructure", the underlying category therein called "Tools", and the subcategory of "Forensic Analysis Software."

A related concept is the verification of data, not because of potential flaws in the tools, but because of the human factor in the investigation process. Two participants expressed this

concept as “peer review” or a practice, standard, guideline or policy that requires that the work of one investigator be reviewed by another investigator for data verification and validation.

> “*..we have the two forensics analysts that conduct analysis and we also do peer reviews to make sure that everyone…all analysts they have…they followed all the standards, they didn’t miss out anything… so it’s important to have peer reviews in the investigations*.” (11CTINTUAE14, p.9).

> “*So, it’s about qualifications and training and appropriate peer review within that laboratory*.” (14ETINTUK14, p.4).

The participant in interview 11CTINTUAE14 explained peer review in terms of a “standard”. The concept of peer review is also discussed in interview 14ETINTUK14 in terms of “qualification” and “training”. The data can be interpreted that the concept of peer review relates to two areas in the research. First, it relates to the core category “Policy” as peer review is about following a standard or policy set within the DFO. Second, the concept of peer review also relates to the core category “People”. The concept of peer review, like the concept of tools, also related at the dimensional level as it implies a minimum requirement of two investigators to review each other’s work or findings.

6.2.3.2 Chain of custody

The subcategory of “chain of custody” appeared repeatedly in the data. Participants explained the investigation process within the context of maintaining a documented record of chain of custody. The data highlights the importance of chain of custody in the investigation process. In interview 07COINTUAE14, the participant stated as follows:

> *“…first of all, I would just keep the chain of custody…”* (07COINTUAE14, p.17).

And participants discussed the chain of custody in relation to the admissibility of evidence. For example, in interview 08SLINTUAE14, the participant highlights the importance of chain of custody with regard to maintaining the integrity of the data:

> *"…basically, you do not preserve the integrity of your data, you do not provide proof that you preserve the integrity of the data during the investigation, then all your investigation means nothing at all…So, of course, under that will come, you know, integrity, you know, chain of custody."* (08SLINTUAE14, p.23).

Two other participants explained how the chain of custody works in practice during the investigation process. These explanations show that chain of custody goes to the heart of the investigation process.

> *"For instance, if we have a disk that we can't get into, and we give it to a company that we know to say can you repair that disk, it's damaged, we want to know what the data is. We would state that that's what we've done, and the person that we've sent it to would come and give evidence, if necessary, saying this is what I did to the disk to make it work and then I handed it back again. So, there's a complete chain of evidence from the point when it was seize."* (05BJINTUK14, p.14).

> *"…the chain of custody record, should mention what is the advisable next step. So, let's say that if this mobile is on an unlock, I would say on the chain of custody, this mobile should be acquired within the next six hours because it will die soon…This faraday bag will eat its battery…This mobile will die soon. So the next person receive it and read the chain of custody, sign it, and add his note…"* (07COINTUAE14, p.18).

The participant in interview 13NXINTUK14 also discussed chain of custody as relating to the concept of vulnerability to "legal challenge", the subcategory discussed next.

"Chain of custody is always…chain of custody is probably the most vulnerable but it's not actually the most difficult to get right…" (13NXINTUK14, p.12).

6.2.3.3 Legal Challenge

The data that emerged into concepts that unified under the subcategory "Legal Challenge" arose mainly from answers to the question the researcher posed regarding the part of the investigation process most vulnerable to legal challenge. For example, in interview 07COINTUAE14, the researcher asked the following question:

"Which part of the investigation process you feel is more vulnerable to legal challenge and why?" (07COINTUAE14, p.22)

Four participants identified the preservation and acquisition as the most vulnerable to legal challenge, as follows:

"First part of course the preservation and acquisition…because it has interaction with your suspected person or the victim. So, if you are a policing entity and you are doing the acquisition always from the legal point of view, this part is the most part that getting attacked from lawyers. They always say that the acquisition was not correct, the data was manipulated and they try to fail the case." (07COINTUAE14, p.22)

"The preservation…because if you left a fingerprint in the physical world, you cannot say no, this is not mine but in the world of the computers, they can say in court, for example, this can be faked. The evidence that you are provide can be faked …" (12CTINTUAE14p11)

*"Probably in the acquisition of the data…so preservation hasn't been tampered with before…"(*09MDINTUAE14p16)

> *"It is always evidence collection. We have seen a lot of evidences which were very accurate and they know accusations to specific people and then the evidence is not, for example, some groups, only one bit of design has changed or something on a phone and we couldn't preserve the evidence and the evidence is considered totally not admissible in court."* (10KSINTUAE14p14)

One participant gave a broad statement that the process and not the produced evidence are vulnerable to legal challenge:

> *"…I think the biggest, the most fundamental part is the process that's been used, the procedure that's been used. So it's the process that's always vulnerable not the, I would say not necessarily the actual production."* (14ETINTUK14p36-37*)*

To the contrary, another participant stated that it is the findings that are "sometimes" vulnerable:

> *"I think it's the findings sometimes." (*16WPINTUK14p23*)*

From the response, one could reasonably conclude that it is the acquisition and preservation phases of the investigation process that is most vulnerable from legal challenge. More specifically, it seems that the legal challenge the participants identified as the source of the challenge deals with the authenticity of the data, whether the data has been "manipulated", "faked" or "tampered". Interestingly, this issue relates to the chain of custody concept, which relates to the category of tools, as explained by one participant:

> *"So, the main thing during forensics is that you need to work on the evidence, work on the file you're doing forensics on without changing anything, right? To keep chain of custody, do not change anything, dates, values on the media, right? So, basically write blockers ensure that wouldn't happen. So, they prevent anything being written on the hard disk…" (*08SLINTUAE14p7*)*

6.2. 3.4 Qualification

Another subcategory that came under the "evidence admissibility" category is that of "qualification." The concept of qualification deals with the staffs that carry out the imaging and analysis, usually the DF investigator who has to testify in court either as an expert or to authenticate the data evidence. One participant explained this issue as follows:

> *"…usually what's also…ahm…challenged legally is your, your value as an expert witness, your background, are you suitably trained, are you the right man to do the job…"* (13NXINTUK14, p.12).

Additionally, there may be an issue with the qualification of people who handled the evidence, which a participant described as follows:

*"…there is a complete chain of people who are responsible for that exhibit…" (*05BJINTUK14p14*)*

6.2.3.5 Pressures

Although the concept of "pressures", which consists of phenomena that impact the investigation procedure or as an intervening condition, may be categorised under other categories like investigation process or investigation procedure. The researcher decided to categorise it under the category "evidence admissibility" because the effects of the pressures is one of the admissibility of the evidence. It is clear, however, that the subcategory "pressures" affects multiple categories across the research, including concepts related to infrastructure and tools, policy, and people. The concept of "pressure" cuts across multiple categories because the most common type of pressure identified by participants is "time constraint", followed only by pressures imposed by people or third parties, and the volume of work.

The majority of participants explicitly identified the lack of time or time constraint during the investigation process as the biggest pressure or challenge to the investigators. The participants were asked slightly varying questions related to challenged or pressure, for example:

"What was the biggest challenge?" (05BJINTUK14p5)

" Is there a particular pressure on this process?" (07COINTUAE14p19*)*

The majority of participants stated that it is "always time" as follows:

*"…finding enough time because we got, I got more work than I could deal with…Time." (*05BJINTUK14p5)

*"It's always pressure of time…Sometimes you cannot do the job at time." (*07COINTUAE14p19)

*"So for us, it's always…time is definitely one. I mean, in the end, we are providing a service to the client. We need to be able to answer the questions that they have within a reasonable amount of time." (*09MDINTUAE14p15)

That participants identified "time constraint" as the most common type of pressure speaks volume about the DF industry and the process and procedures used, but most importantly about what DFO capability should mean. The researcher posits that capability, if a standard is to be agreed upon, must be determined keeping in mind the amount of time an investigator has to conduct a full investigation. In other words, "throughput" must be measured (Jones and Valli, 2011).

Time constraint also relates to issue of policy and procedure and case management since issues of time, as identified by a participant, depends on the case:

"It depends on the case because some cases require have the minimum time." (12CTINTUAE14p10)

What becomes necessary is a capability in the DFO to control the resource of time so that the pressure of time does not significantly affect the investigation process. One participant explained the issue in relation to human resource management through overtime and hours worked and in relation to a policy or procedure of managing client expectations of time:

> *"Oh yeah, because everybody wants their case done first, and that's the pressure that you get. It's not pressure in relation to the actual work…Time. Yeah. You know, there's only twenty four hours in a day. And everyone wants you turning eight …What we used to do, we did some amounts of overtime because there wasn't enough of us. And eventually they realized and they started to build the department up a bit. But no that is one of the biggest pressures in terms of time and trying to manage expectations when a job comes in. Don't give them the impression it's going to be done next week."* (15RMINTUK14p42)

Another participant expressed the pressure of time in relation to the volume of data, creating multiple types of dimensions under this subcategory: "amount of time", "rate of throughput" and "size of data". The participants explained that the pressure of time is relative to the pressure of "volume of data" growing over time.

> *"There was always pressure. Time is always a pressure. Volume of data would becoming increasingly a problem …it comes down to the time thing but the same expectations were placed on you five years ago as what would be placed on you now. The difference is there's a lot more data than what there was five years ago. So there was pressures there."(*13NXINTUK14p11*)*

Aside from the pressure of time during the investigation, participants also identified pressure related to people or third party. These types of pressure vary depending on from the role of the third party as a client, a supervisor, and others. One participant, for example, identified the coroner as being able to create pressure in the public sector:

> *"…it depends on what type of case it is, but there might be court pressures, it might be a coroner's inquest…" (*16WPINTUK14p21*)*

Of course, in the private sector, one of the biggest sources of pressure is the client, who pays the investigator to do the DF investigation. The pressure range from managing client expectations, client communication, finding results, and time:

> *"So first pressure is gaining the client trust that he can actually trust us to do this investigation. The second thing is making sure the client understands what could be the outcome of this investigation. You know, the clients you go to are not always tech savvy or law savvy in that matter. So they expect after this investigations you will identify this is the issue, this user did this and you will give them a complete suspect and accuse him. But that's not the case. So in many cases where you do not find who did it, you know what happened but you cannot find who did it cause you know these customers lack certain controls in place that can trace the issue or trace whoever did that. Right? So, second point is, you know, we make customers understand the outcomes, the possible outcomes and what they might get from this investigation, So these are the two initial points."* (08SLINTUAE14p19*)*

> *"And also outside of the criminal area, in the civil sector, there's lots of pressure from the client. They after all are paying you to do your job. When they want it done quickly. They want you to find the right result for them and that's not necessarily…you might not find the right result for them, and that is a pressure because they are sure that something's happened and you are sure that something hasn't…"(*13NXINTUK14p11

Coming up with results, therefore, can be a pressure that can be troublesome if the client's expectations are not managed, because an investigator cannot and should not invent data that does not exist. Yet, truth may be a pressure as well, as the following participant states:

> Question: *"…which is the most difficult part of investigation?" (*05BJINTUK14p27*)*

Answer: *"Finally, the truth." (*05BJINTUK14p27*)*

The pressure for results also relates to the investigation process and whether an investigator may deviate from it in order to search deeper for results that was not found after an initial search.

> *"And results… When you have the evidence, you can't find the evidence. You try, you try but you can't. So you have to think outside of the box. How can I find more results, how can I dig deep and search more or do we need more evidence?" (*12CTINTUAE14p11*)*

The pressure from "results" relates to another type of pressure to the investigator, which is the pressure to keep the integrity of the data, or the data's authenticity and reliability. This pressure counterweights the pressure from client expectations on results. An overarching requirement that relates to the investigation process and the DFO's procedures is maintaining a documented record of the chain of custody and the procedures used in the DF laboratory and DFO. Integrity of the data is a pressure that possibly affects all other categories. One participant noted the significance of this pressure:

> *"…basically, you do not preserve the integrity of your data, you do not provide proof that you preserve the integrity of the data during the investigation, then all your investigation means nothing at all…So, of course, under that will come, you know, integrity, you know, chain of custody." (*08SLINTUAE14p23*)*

6.2.4 Tools

Tools and technology are an integral part of DF investigation. The use of tools makes the DF investigation more efficient. Tools make DF investigation easier and faster, and a DFO cannot function without at least the basic tools at hand. However, one participant explained the relationship between tools and people, specifically that the skill of certain persons may be more powerful than tools:

*"Probably, somebody to be able to do it manual would be very nice because in our practice we have found out that manual evidence analysis always finds, without any exception, always finds more information than any tool available. Because what is a tool? Tool is a set of routines programmed within that suite of activities. It asked, do these take evidence from these folders, gather it, don't write, you know, cutting the right portion, write-protect. Take it, copy it, make an evidence file of, for example, any, custom file or whatever. Save it here. Name it Evidence One or whatever name. And then analyse, but this doesn't happen in manual analysis. Manually, an engineer is looking at what is available. He's not just looking at the folders that I have, just look at these folders. No. We actually have to look at different folders…" (*03ALINTUAE14p10-11*)*

*"The software that you're using it doesn't really matter what software you are using if you understand what's going on behind the scenes."(*09MDINTUAE14p4)

The category "Tools" deal primarily with two subcategories of tools used in DF: software and hardware. First, this section discusses the subcategory "tool selection" as it affects the discussion on software and hardware tools. Second, this section discusses the different types of forensic analysis software used by the participants. Finally, this section shows the types of hardware used by the participants.

The first subcategory that emerged and became part of the "tools" category is "tool selection", which are concepts and phenomena described by participants regarding the factors they take into account when choosing tools for their DFO. In this subcategory, however, most of the statements were about the forensic imaging and analysis software, particular why participants chose Guidance Software Encase or Access Data FTK. Even the follow up questions during the interviews ended up focusing on this issue as follows:

> *"So, when you guys chose Guidance, was it because of business requirement or because of financial reason or because of its efficiency?" (*08SLINTUAE14p8*)*

The participants' response shows that the choice of using Encase or FTK was because these two are the leading software analysis tools in the DF industry, and what if some participants even referred to as an industry standard:

> *"They are the industry standards. Everyone uses them, so we have to be able to read and write in their formats. So really, for me, it's a case of having flexibility to use the tools. It would be…if I only used one tool, it would be a bit like a car mechanic only having one spanner. You have to have a range of tools. So for me it's flexibility and the ability to compare results between the tools." (*14ETINTUK14p15-*16)*

> *"…we found that Guidance had the best range of software. So, they covered from small to large enterprises. They cover individual forensic as well. So, that's why the decision came to Guidance and, you know, they're very well known in the industry. They have annual conferences in the U.S." (*08SLINTUAE14p8*)*

That EnCase and FTK is industry standard is certainly subject of controversy, but it would be interesting to note, perhaps in future research, what percentage of the industry agrees with this statement.

What also seems to emerge from the data is that peer review using multiple tools is a necessity, and so is the capability of having tools that meet the DF investigators' tool preferences. The subcategory of tool selection, therefore, relates to data verification and validation discussed previously. Furthermore, having both FTK and Encase, and perhaps other tools, may be necessary for a DFO's capability. One participant described the phenomenon as follows:

> *"So, we just don't trust one particular tool. We just don't go to Encase and do the investigation. No. We would use Encase. If it's very important project…I'm sure in terms of police investigation it is always important. When real crime has happened. So, we would use Encase. We would use other tools." (*03ALINTUAE14p10-11*)*

It is also important to select tools based on the DF investigator or analyst's preference, as stated by the following participant:

> *"So it's more the tools are available and depending on the analyst preference you want to enable the analyst to do the job accurately and as fast as they can to provide the proper results. If you happen to prefer FTK over Encase, then use FTK over Encase." (*09MDINTUAE14p6-7*)*

The other factors that participants raised for tool selection concerns are the performance of the tools and the purpose for its use.

> *"It depends on the case." (*12CTINTUAE14p3*)*

> *"It's because of efficiency and it's because of performance as well. It's not about finance. The equipment….our concerns for the equipment is that it makes our job easier from a forensic point of view." (*05BJINTUK14p6*)*

> *"Well, usually, we try to use the tools with the least impact on the system." (*10KSINTUAE14p5*)*

The subcategory "tool selection" came from concepts that emerged from the data and which make clear the relationship of tool selection to other categories, concepts, and dimensions. Tool selection, for example, relates to standards and policy with regards to determining whether Encase and FTK are industry standards in tools, and whether there is a need for multiple tools. Tool selection also relates to the investigation process and

procedures and to the skill of people use them in the DF industry. Tool selection, therefore, should be considered, taking into account other concerns in other categories and subcategories.

6.2.4.1 Forensic Analysis Software

Another subcategory that relates closely to the Tool Selection subcategory is "Forensic Analysis Software." There were three types of forensic analysis software that emerged from the data. First, participants discussed the standard software used in DF investigations. Three stood out as leading in the industry: Access Data FTK, Guidance Software Encase, and Xways. FTK and Encase were already discussed previously under tool selection, but when participants were asked the question,

> *"What are the commonly used digital forensic tools in terms of hardware and software?" (07COINTUAE14p6),*

Xways also starts appearing as an up and coming challenger as a standard in the DF industry. Second, participants discussed malware analysis software as a tool used in DF. Finally, participants discuss the use of open source tools as a supplement to the commercial tools like FTK and Encase.

6.2.4.1.1 Standard tools: FTK, Encase, Xways

Participants were asked the following question and the result was that the majority gave similar answers:

> *"What are the commonly used digital forensic tools in terms of hardware and software?" (*07COINTUAE14p6*)*

Participants almost unanimously indicated their choice for FTK, Encase, and/or Xways. Other tools did emerge as well but usually in addition to one or more of the first three.

> *"In analysis, I would say the most common used to come up with computer forensics now, I'll say Access Data FTK or Guidance Encase or Linux*

*investigation. These are the three ah…top applications we use around the area. There was other applications to be used but it is from my perspective I can see that if I have Encase forensics I can do any investigation that I have to do. If I have FTK I can do investigation I have to do but there is some tool specific to one purpose…" (*07COINTUAE14p7*)*

"Encase, FTK, Xways Forensics…Those are the three main tools that we use which are commercial tools, yes." (05BJINTUK14p7)

"…You got your AccessData, you have your Guidance, then on field…XWays…" (09MDINTUAE14p5-6*)*

*" …in terms of computer examination, our most common software will be Encase and FTK, although we've just been trained on Xways." (*16WPINTUK14p8*)*

*"Well, they're [FTK and Guidance] the most common tools…ones I see a lot more in Europe, mainly is a German tool is Xways...the easiest to use is FTK…The next easiest is Encase and the hardest to use, because it's all in Exodus and all, is Xways… Wherever I go, I don't think there's favourites, I always ask people on every course I run, you know, what's your favourite tool and without a doubt it's either Encase or it's FTK. And it really just suits the individual, how they work really, there are hardly any two major manufacturers of forensic software anyway." (*15RMINTUK14p21-22*)*

*"For the software tool, we use the NF and the most famous one, FTK. We use Encase and we use other tools that can help us…we can use VMWare to analyse dynamically the image of the computer if it was handled as an evidence. We use other tools that can analyse the loops." (*12CTINTUAE14p3*)*

The forensic analysis tool used for mobile phone, XRY, was also mentioned as a standard or "generic" tool. XRY is also discussed more fully below.

> *"The tools we use here are the generic tools…the Encase, FTK. For mobile, we are using XRY… Those are the most common. They're the most common and…I mean, they are the most popular in the market right now…so that other forensic labs like em…the law enforcements are using it…our competitor are using it as well. So, we went ahead with the standard tools…" (*11CTINTUAE14p5*)*

Some participant indicated the same standard forensic analysis software but explained their preference among the three:

> *"…FTK. One of the reasons is that it does allow for one set of evidence, and two sets of this data. It's really a network tool… FTK is very useful for cases where you are going to bring in investigators." (*15RMINTUK14p16*)*

> *"… but most of the time, Guidance can deliver everything that we….Our open source tools are used if we have some platform that Guidance did not support which used to be in the past like mobile devices…some iOS versions. But then afterwards, they came with this capability and we simply did not need…" (*08SLINTUAE14p8*)*

> "*…And of course you have the Encase, which is quite popular commercial tool…*" *(*10KSINTUAE14p4*)*

Notably, one participant went as far as saying that Xways is better than both FTK and Encase, an indication that Xways may be on its way to contend for the market lead in the industry.

> *"…so we use Encase. If you want versions I can give you versions. We use 619, I think, we haven't gotten to Encase 7…We use FTK, 4. It is the core tools…But my primary tool now is Xways…Which is much better than both of those put together…They are the industry standards. Everyone uses them… And we have to*

*be able to take on a case that somebody else might have done in Encase and review the results in Encase. But we also need to be able to do what we call jewel tool corrupt corroboration. So, if I've got a case done in Xways and I've found some results. I will do the same job, look at that data again with Encase to make sure that I get the same results, so that I can then flick between Encase and FTK, Xways and Encase, FTK and Xways. So I can use the tools interactively, and some tools are really good at some things and some tools are really good at others." (*14ETINTUK14p13-15*)*

What becomes clear from the emerged data is that DFOs may be required to have all the standard tools in the industry for purposes of data verification and validation, and for allowing ease of cross-platform use. Capability in terms of forensic analysis software, therefore, takes on a highly specific dimension, and it looks very possible that an industry standard may be achieved in this regards.

Of course there will be arguments regarding preference and the ability to use other software. Such positions are not necessarily wrong, but the point for having a standard or a baseline for what capability means in terms of software tools largely means being able to analyse data across a set of software that will be readily available in the industry. Of course, such a standard should not be set in stone and could change over time as shown by Xways.

6.2. 4.1.2 Malware Analysis

The topic of 'Malware analysis tool' also emerged from the data. However, none of the participants indicated that malware analysis is an industry standard. Rather, malware analysis may be necessary when a case may require it. In short, malware analysis software is a good addition to tool capability as described by the following participant:

"… We use also malware analysis because sometimes in the forensic case, you can have an infected computer that lead to that incident. So that could be stealing something. That's why we can also analyse the malware to know the activity of it.

*Where does it send this information? How does it do it? And we can have information on that" (*12CTINTUAE14p3*)*

6.2.4.1.3 Open Source Tools

A number of participants also indicated that they use open source tools to supplement existing tools. No participant indicated that open source tools without commercial tools are sufficient. Instead, open source tools were viewed as a way to enhance capability in analysis software. The participants were asked the following question:

*"Did you guys consider open source tools as well?" (*08SLINTUAE14p8*)*

The replies by the participants revealed an acceptance of open source tools in the industry:

*"Yeah. Sometimes, we need to…we do use open source tools…"(*08SLINTUAE14p8*)*

*"…yes we do sometimes, but we also use commercial tools. Open source and commercial." (*05BJINTUK14p6-7*)*

*"Yes, we do use open source, commercial and internal tool." (*10KSINTUAE14p6)

*"Yes, we do. For…cause open source sometimes they cover specific, specific related tasks. For example, when we retrieve email from Exchange, there are some open source that help us retrieve the email and later of chronological order. Sometimes when you do, when you want to restore some defected information from hard, some hardware, open source tools also can help with that." (*11CTINTUAE14p5*)*

"…we have and we will. We've not really got a massive issue with using it, but the problem is as we've already discussed this, twelve thirteen of us…when do we have

*the time to do the research to be able to say, yeah, this tool is good enough for us to use." (*16WPINTUK14p9)

*"I do a lot of my stuff using the open source tools, specifically with the reason that I can automate those, get scripts around the problem and I can get the results quicker than using a software like Encase." (*09MDINTUAE14p7*)*

6.2.4.2 Hardware Tools

The second type of tools under the category "Tools" was grouped under the subcategory "Hardware." Unlike software tools, the participants did not identify specific brands used for hardware. One participant stated the following:

*"I mean the hardware is really up to you." (*15RMINTUK14p16*)*

Instead, participants focused on describing the type of hardware used. These types of hardware included the forensics workstation, storage devices, peripherals and accessories, specialized DF tools like write blockers, imaging, and duplicators, and hardware used in small scale device investigations.

Participants indicated the need to have a forensic workstation, which may be specialized according to a DFO's requirement.

*"…so, any lab that we have is gonna look more or less the same, including the hardware we are using...as far as computer hardware goes specialized forensics workstations obviously…there are a couple big players out there…"*09MDINTUAE14p2*)*

One participant explained the need to build a forensics workstation, though it might have been because it was done a few years ago.

"…we build our own machines, forensically. So, we built at a very high performance forensic machine which has got slots in so you can take a hard drive,

slot it in, perhaps with the right locker, push it in to the unit and…we've got about three or four machines that have…which are all high performance forensic machines we built…Because the machines that are bought…domestic machines which are bought are not good enough for forensic work.."(05BJINTUK14p6)

One participant identified some of the accessories needed in a DF laboratory as well:

*"…hardware? Byte walkers, of course, drive erasers, specific than work stations port that will support various connectors essentially on the box to speed up to speed up things…we're talking, if we're looking at a bread box which I've seen on my pass link, SATA bridge, SAS bridge, all, all, all the connectors that you essentially can manage to connect to whatever you have when you're on the field. And, of course, a lot of CPU power around and just a place to do the analysis…" (*09MDINTUAE14p6*)*

6.2.4.2.1 Write blockers/Imaging/Duplicator

One of the most important types of hardware that often emerged from the data was the need to have write blockers, imagers and duplicators. These tools are important because they go to the heart of what DF investigations do: prevent alteration to digital evidence using a write blocker, preserve digital evidence by imaging, copying or duplicating the digital evidence using the duplicator, and analyse it using the copied version without altering the original data and without allowing any other alteration to the original data. In essence, write blockers, imaging and duplicating tools are essential tools. One participant stated the necessity as follows:

*"So, main component is having write blocker and duplicate them. That's your basic requirement to do any forensic capability, okay?" (*08SLINTUAE14p6*)*

*"…one element to it is just hardware…needed to get hardware in place such as servers, write protection equipment, etcetera." (*08SLINTUAE14p6*)*

Even with forensics done in the field, the same tools will be needed:

> *"So, you must have forensic tool kit bag so, which will include your mobile write blockers, your fast duplicators. So, you can on the spot, if there is a remote place…you can go to and quickly take a snap look at that system." (*08SLINTUAE14p9*)*

One participant went further and identified the brand of the hardware:

> *"...And then in the hardware, if you need to know hardware as well?... All of the Tableau range. Voon V-O-O-N. Which is a write blocker. Very old now. Spectre, of course, which is our own tool. We use that a lot." (*14ETINTUK14p15*)*

Additionally, participants stated the need for a server or database:

> *"…you got a database and that can either be Oracle or Microsoft Secret Server or Postren which is a free one." (*15RMINTUK14p24*)*

6.2.4.2.2 Small Scale Devices

Finally, participants identified the need for hardware in conducting DF investigations of small scale devices like mobile phones. These tools were categorised under hardware despite the fact that they are sometime mixed hardware and software. Regardless, two small scale device tools commonly emerged from the data were Cellebrite and XRY. Both are common in mobile phone investigation. One could, therefore, conclude that a DFO that engages in small scale device forensics must have these two tools, as minimum, among other tools.

> *"And then for phones, you're gonne be doing smartphones?...Two. There's cellebrite. And then the other one is XRY, the Swedish one." (*15RMINTUK14p26*)*

> *"For mobile, we are using XRY." (*11CTINTUAE14p4*)*

*"For mobile phones, we've got Cellbrite, we've got XRY, we've got a number of tools. We don't, we don't just do one, depending on the phone, the state it's in. We've got, you know, a handset at hand, a load of tools that can assist us to get into em." (*16WPINTUK14p8*)*

Additionally, one participant uses Oxygen, and another mentioned the use of a Faraday bag, which seals the mobile phone from any wireless access.

*"We've got Oxygen, we can do chip-offs, we've got capabilities for chip-offs.. "(*16WPINTUK14p8*)*

*"There is for mobile investigations specifically there is acquisition solutions like Faraday bags…it's mainly to isolate networks so if you are doing an acquisition for a mobile device that can be remotely wiped." (*07COINTUAE14p9*)*

6.2.5 Cloud Environment

An increasingly important area of DF is cloud computing. This section discusses the cloud environment, as described by participants, as a potential for adding to the DF infrastructure and organisational capability. In this regard, the participants were asked the following question:

"Do you use cloud environment?" (03ALINTUAE14p16)

The participants' responses were then grouped according to concepts that pertained to four subcategories: "cloud platform", "cloud storage", "cloud processing" and "cloud security".

6.2.5.1 Cloud Platform

The majority of participants were against the use of the cloud as a platform, as is apparent in the responses. One participant was asked the following question:

*"Neither use it for as a platform?" (*08SLINTUAE14p10*)*

The participant stated as follows:

> *"No, no. You know they say cloud is stable and fine, but we don't". (*08SLINTUAE14p10*)*

> *"I don't think that would be good idea because cloud not safe with us. Alright, we can exclude in case the job was hosted within the process." (*12CTINTUAE14p5*)*

One participant indicated the use of cloud as a platform, not to conduct for an investigation rather as a research tool for reverse engineering.

> *"Yes. We use cloud. …this is as a platform. We use it basically as an R&D. We use it to find the weaknesses in the cloud." (*03ALINTUAE14p16*)*

Another participant indicated the potential of using the cloud in the future:

> *"…no not at the minute…Yes there is future plans. We've got huge data centre at the minute, so they're discussing cloud but til they can tell our IT department…til they decide what they want to do, …we've got our own servers and we back up to em our data centre." (*16WPINTUK14p9*)*

6.2.5.2 Cloud Storage

The majority of participants were also against the use of the cloud as a storage medium. The participants were asked questions about cloud storage like the following:

> *"In your investigation, you use cloud also to store your memories, data and all this?" (*10KSINTUAE14p7*)*

The participants replied negatively for using cloud as a storage medium for DF investigation data because of the security concern with the cloud, and the ease of access to the data on the cloud:

*"…most probably not." (*10KSINTUAE14p7*)*

*"Cloud? No, no. We don't store anything on cloud." (*08SLINTUAE14p10*)*

*"No…We cannot use local storage in the lab." (*11CTINTUAE14p6*)*

Another participant explained that the issue with security is also an issue of unnecessary exposure to security risk when there are least risky alternatives:

*"No...for our lab, it's totally isolated even from our network…Okay, it's not like we cannot secure it. Of course we can secure our data even if it's on the cloud…but why do I need the extra headache for securing my data on the cloud while I can just keep it inside? If there is requirement to my client to use the cloud, then I will go for how to secure it. How do I secure my data and how do I get assorted or assured that my data is secured on the cloud." (*07COINTUAE14p9*)*

Two participants stated that cloud storage would not be sufficient for the type of storage space needed for their DF investigations:

*"Cloud storage it would not be sufficient..." (*12CTINTUAE14p5*)*

*"We do use some cloud based on other parts of the company but for forensics it's just it doesn't work with, you know, you, you're dealing with large data sets. It takes time to upload download these and it's hard to work with if they were on the cloud." (*08SLINTUAE14p10*)*

6.2.5.3 Cloud processing

There were two participants who were open to the possibility of using the cloud for processing rather than as storage or a platform to add to the speed of their tools.

*"No. I might use the cloud but in a different way. I might use cloud processing if I need to have more processing power, I can use cloud processing but cloud storage I don't see it feasible." (*07COINTUAE14p9*)*

There remains concerns; however, regarding control of the data that goes on to the cloud and that such use may violate accreditation standards like ISO.

*"…cloud processing yes it would be but it's not a good as it was with Amazon, NWS or any other cloud provider because the data would be not with our premises. …And if it's not…it's against the accreditation on the ISO standard." (*12CTINTUAE14p5*)*

Instead, the participant raised the possibility of creating a private cloud as part of the DFO capability. It would be the cloud that is privately used by the DFO and remains isolated from the public or any third party unless authorised by the DFO:

*"For me it would be a private cloud though. Our challenge would be…you could go with somebody like Amazon and have an E3, for instance an E3, which would be great cause you know it's gonna be there, but you don't know…you have very little control over the relationship between you and Amazon. Amazon are much bigger than us. So if they said we're not gonna bother servicing you anymore, they could…or they could say we've just sold to Mercedes Benz, so suddenly you got a supplier change and we don't know what their policies are about allowing forensic images on cloud. The other problem would be, some of our data is so sensitive, some of the data we handle is so sensitive, we have to almost physically have our eyes on it." (*12CTINTUAE14p5*)*

6.2.5.4 Cloud Security

As shown above, the greatest and underlying concern with its security. Since the DF industry deals with the sensitive and criminal investigations, security of the data is very

important. So, when asked why participants did not use cloud, the common response was due to security:

> *"Yeah. Specifically that we are working with customer data and we don't want to add any level of exposure to the customer that is not essentially dependent on us." (*09MDINTUAE14p7*)*

> *"I don't think that would be good idea because cloud not safe with us."* 12CTINTUAE14p5*)*

> *"It's all about security is also up to them to authorize us." (*16WPINTUK14p10*)*

> *"Under no circumstances. Don't go anywhere near it…Oh no, no, no. Certainly not. Too dangerous…It's too insecure….It's a matter of security. After the task or the job that we do, we are given, is very, very sensitive and there is no way…and often, for example, when you're carrying out that process, I mean, sure you're disconnected from the internet, so it's no possibility of leakage from what you're doing. To use the cloud would be totally wrong." (*05BJINTUK14p7-8*)*

One participant pointed out the relationship between the concern for security and making the prohibition on the use of the cloud a policy of the DFO:

> *"So…no. …that would be one of the things that we definitely do not, so again, that's our policy. We have data storage in the labs. We have tools in the labs we use…I'm storing data related to cases…no problem." (*09MDINTUAE14p7*)*

The category "cloud", as can be seen from the responses above, also relates to other categories like policy, tools, and even the investigation process. Issue of security with the cloud raises awareness with security and data storage policies, among others. Cloud also

raises issues related to the use of cloud as a tool and how it may hinder or enhance the investigation process and capability.

6.2.6 Building a DF Facility

Participants discussed various concepts relating to the category “Building a DF Facility”. Most discussion regarding building a DF facility related to the capability and experiences the participants had in actually setting up a DF lab. This section have grouped the concepts discussed with the participants divided into five subcategories: “process”, “facility requirements”, “security”, “financial”, and “functionality and scope”.

6.2.6.1 Process

Participants talked about the process of building a DF lab. The process is not simple and requires a number of phases, including requirements analysis, a design phase, client consultation and approval, determining the scope of the lab and the DF services the lab aims to undertake, the physical infrastructure, the setting of standards, security of the DF lab, and both physical and digital storage. It is a concept that requires more detailed study, and could perhaps lead to further research in the field. One participant explained some of the phases of the lab building process as follows:

> *“Yeah. So, normally what we do…we have a start-up meeting where we meet with the client and identify the requirements. So, we start getting what really do they need, what they want to have as a result of this project. And then we do design phase where we start meeting this requirement with matched solutions and so on...and then we go again for approval of this design and we describe what will be the result of implementing this design…And then we go for the delivery…the project delivery where we start implementing…doing the setup and so on.” (*07COINTUAE14p3*)*

Another participant explained the process of building a DF lab in terms of requirements and capabilities:

*"If you're designing a lab from scratch or working on one in your country. They want everything. They want the ability to receive evidence, process of evidence both computer and cell phone evidence, fixed physical storage. They also want the ability to disassembly, physical, physical recovery, and training. So those all those parts play a part in the design of the physical lab. So, once you've identified what it is you want to do, you then have to identify the physical premises that will allow you to do it. Then you can identify any changes that are required to the physical premises to allow you to obey the standards. So, continuity, security, EXT protection, CCTV, secured storage, fire suppression, all of these things are the first steps in identifying how to build a forensic laboratory." (*14ETINTUK14p4*)*

6.2.6.2 Facility Requirements

Another subcategory is the "facility requirements." One participant viewed the facility requirement as the most important issue when building a lab:

"*But for me, facility is the first one. The cost is a big one." (*14ETINTUK14p12)

This is understandable as the facility requirements involves numerous considerations which emerged from the participants' answers as "tools and equipment" in a facility, "people" or "staffing" the "facility", the "size" of the facility, and the "physical infrastructure." One participant described the elements of building a DF facility, which involves the tools, equipment, procedures, and the physical lab itself.

"Yeah. There's a number of elements to it, one element to it is just hardware…needed to get hardware in place such as servers, write protection equipment, etcetera. Software…identified a number of different tools and suitable for different tasks and also able to jewel tool as well. So, if I had one task and it was….sorry, if I had one tool that was able to do X, I need to get another tool that could do X as well, so I could jewel tool. And then the other elements, there's obviously staffing. So, I had to go out there and do a lot of recruitment, a lot of

background checks, etcetera. And then importantly building standards and procedures. I built a lot of standard operating procedures, so when we were bringing staff into the unit, they were working to a consistent output, if you like. And they were working toward a consistent output. And then finally, building the physical lab itself, had to get controls in place to make sure only specific people could go in the lab, etcetera." (13NXINTUK14p2 *)*

Additionally, there was a need to staff the facility.

"…and then the other elements, there's obviously staffing. So, I had to go out there and do a lot of recruitment, a lot of background checks, etcetera, etcetera." (13NXINTUK14p2 *)*

*"…obviously you need the physical equipment to make technical capabilities, but you also need to have the human resources able to do it."(*14ETINTUK14p4*)*

One participant, however, did not view staffing as a challenge:

*"So…now that's interesting because I would find it easier to find the right people. There are a lot of people around but it's still a challenge finding, in any environment, finding the right staff to work the way you want to work…"(*14ETINTUK14p11*)*

Another concern with building the facility requirements was the physical building structure itself and whether it would include certain areas like a research and development (R&D) wing:

"*And then finally, building the physical lab itself..." (*13NXINTUK14p2*)*

*"…I think R&D facility would be an essential part of the coming forensic capability of any organisation, especially big ones…" (*03ALINTUAE14p8*)*

Finally, the facility requirements also needed procedures in place to manage people, standard and procedures regarding building, standard operating procedures, and technical manuals for those conducting the investigation.

> *"…had to get controls in place to make sure only specific people could go in the lab, etc. . ." (*13NXINTUK14p2*)*

> *"And then importantly building standards and procedures. I built a lot of standard operating procedures, so when we were bringing staff into the unit, they were working to a consistent output, if you like. And they were working toward a consistent output." (*13NXINTUK14p2*)*

> *"And they must to follow the technical manual…ah…for, for all, for all procedures undertaken in the lab." (*11CTINTUAE14p2*)*

The subcategory of facility requirements, therefore, was also related to other categories as facility requirements encompassed concerns related to people, tools, policies and standards,

6.2.6.3 Security

Another subcategory that emerged from the data is "security." A participant indicated that security was part of the consideration when building a DF facility:

> *"So, continuity, security, EXT protection, CCTV, secured storage, fire suppression, all of these things is the first steps in identifying how to build a forensic laboratory." (*14ETINTUK14p4)

> *"…I guess facilities would be third. The appropriate facilities for the work that you're undertaking. And security…physical and logical security. So it's both the*

*physical parameters that you're in…the environment and the steps you take for logical protection." (*14ETINTUK14p10)

6.2.6.4 Financial

Participants also raised the issue of budget and costs when building a DF facility. The financial aspect of building a DF facility is often ignored, yet this has a substantial impact on the capability of a DFO and its DF facility. Two participants stated their financial concerns relating building a DF facility as follows:

> *"…actually the biggest one was financial because it costs a lot to set up a forensic laboratory and keep it running properly. It costs a lot to have the right environment and the right equipment…. The cost is a big one."* (14ETINTUK14p11-12)

> *"It always is a big challenge…because…we had to fight for the budget because typically if it comes under the police heading which yours does as well…everybody is trying to get that money." (*15RMINTUK14p12)

Interestingly, financial considerations relate to all other categories since it will dictate the ability of a DFO to achieve capability.

6.2.6.5 Functionality and Scope of lab

Finally, the subcategory of "functionality and scope of the lab" impacted how the participants viewed the type of DF facility to be built. One participant was asked to identify the key steps to creating capability:

> *"…can you identify the key steps when you built your forensics provision or capability?"* (11CTINTUAE14p2)

The participants answered as follows:

*"Key steps? Well, first of all, identify the scope. So, first we decided that yes, we'll be covering computer forensics and mobile forensics." (*11CTINTUAE14p2*)*

*"So the first step is to identify the nature of the forensic analysis that's gonna be taken. So first, in order to design processes and procedures, the first step is to identify what work you're likely to undertake...The type of forensic work that you're gonna do…If you're designing a lab from scratch or working on one in your country. They want everything. They want the ability to receive evidence, process of evidence both computer and cell phone evidence, fixed physical storage. They also want the ability to disassembly, physical, physical recovery, and training. So those…all those parts play a part in the design of the physical lab. So, once you've identified what it is you want to do, you then have to identify the physical premises that will allow you to do it. Then you can identify any changes that are required to the physical premises to allow you to obey the standards…"(*14ETINTUK14p4*)*

The category "Building a DF Facility" is central to determining a DFO's capability development and management. Examining the participants' views about the elements of building a DF facility is therefore important in determining the meaning of DF capability. What became apparent from the data is that in certain category of building proper DF facility does not exist independently but linked to other categories that involves policy, procedures, people, technology, and the investigation process.

6.2.7 Organisational Development and Management Standards

This section discusses the findings in the data relating to "standards in developing and managing a digital forensics organisation". Two sets of questions were asked here. The first question asked was about the existence of any standard guidelines for developing a DFO:

"Do you know any guideline for developing a digital forensic, a standard guideline?" (05BJINTUK14p1)

A related and follow up question was also asked regarding the existence of a standard for managing a DFO:

> *"…do you know any standard guideline for managing those capabilities?" (*10KSINTUAE14p1)

The participants' answers resulted in identified concepts that were grouped into the following subcategories: "standards", "guidelines", "lab accreditation", and "key success factors".

6.2.7.1 Standards

In the subcategory termed "standards", three types of answers from participants emerged from the data. Majority of participants stated that there is no absolute standard for developing or managing a DFO or DF facility. Participants, however, indicated that the ISO provides guidance, especially with regards to general quality standards. Additionally, participants identified the ACPO Managers' Guidelines as providing guidance, if not as a standard in UK law enforcement.

6.2.7.1.1 No absolute standard for building or managing

The majority of participants made clear that no absolute industry standard exists for developing or managing a DFO or DF facility. One participant indicated, for example, that there is neither a guideline for "setting one up" nor for management:

> ***"****…I don't think there's a standard guideline. There's most definitely some procedures that should be followed once you've set one up. I haven't seen a guideline in actually setting one up in the first instance.… …managing as such…no, the guidelines I'm thinking of really are the guidelines in association with the forensic process and how things process, progress through a laboratory…managing wise, I suppose we, we just again developed on the fly, alright, our management technique" (*15RMINTUK14p1)

One participant indicated that the best practices from vendors served as a guide for developing and managing a DF facility:

> ***"****Honestly, when we started we relied on the…best practices from the vendors…research."* (11CTINTUAE14p1*)*

Participants were specifically asked about the existence of a standard guideline for building a DFC, either as an organisation or as a facility. One sample question was stated as follows:

> *"…basically there is no standard guideline for building a digital forensics. Is there a one way of doing it?"* (11CTINTUAE14p1*)*

Five participants replied that there was no such standard:

> *"No, there is not."* (11CTINTUAE14p1*)*

> *"there's guidelines that's related to it, but there aren't specific guidelines." (*13NXINTUK14p1)

> *"…there's no absolute standard guideline for building digital forensics laboratories…" (*07COINTUAE14p1*)*

> *"Okay. I'm not sure there is a standard guideline. I haven't come up with anything that's standardized in that space, but I believe there are general rules that you follow usually when you are building a forensics…" (*08SLINTUAE14p1)

> *"…I am aware of multiple though I haven't been inside out, no, not to the extent that you probably would if you need to actually set up a full forensics lab according to the policies…" (*09MDINTUAE14p1)

Participants were also specifically asked about standards for managing DF capabilities. One question was posed as follows:

> *"…do you know any standard guideline for managing those capabilities?" (*10KSINTUAE14p1)

Four participants made it clear that no standard for managing a DF capability existed:

> *"No, I don't." (*10KSINTUAE14p2)

> *"No. No, no. Not an industry standard… in the region it's not…you're not required to follow any guideline. So it ends up being, a matter of preference for the company." (*08SLINTUAE14p2)

> *"No standard guidelines, again there's lot of periphery guidelines."* (13NXINTUK14p1)

> *"I don't really know about standards or available guidelines. I know that there are best practices that are available for everyone who are trying. They are mostly based on personal efforts like my organisation. We have a group of people trying to establish like a policies for investigations." (*10KSINTUAE14p1)

One participant also pointed out the lack of standard regarding forensics expert qualification.

> ***"****There are, I said, there is no specific standard to identify forensics experts, so in case you will find a lot of people who are certified but when we go to the lab and actually do the manual analysis or try to find out facts, they are not really experienced." (*10KSINTUAE14p2)

6.2.7.1.2 ISO

Participants resorted for ISO 17025 as a guideline for developing and managing a laboratory, by following the general processes prescribed by the ISO. These participants followed the ISO standard either because they were already ISO certified or because ISO simply served as a general standard guideline.

One participant indicated that ISO may be helpful in developing a lab, though its guideline does not directly deal with DF.

> *"There's also ISO Guidelines on setting up a forensics science lab. Again, not specific to digital forensics, but the concepts are there… there's a couple of other guidelines such as ISO-9001 which is built around quality. It's a general quality guideline but not necessarily a forensic standard." (*13NXINTUK14p1-2)

Most, participants were not aware of or did not rely on the ISO for developing a DFO, instead relied on the ISO as a standard guideline for management and processes in the DFO or DF facility.

> *"There is ISO standard for labs…It's ISO 17025…That's for general lab, even for medical labs environment, how to manage lab environment... And there is a specific other ISO standard which is 17037…And this is for handling digital evidence." (*07COINTUAE14p2*)*

> *"There are multiple standards for information security in a general or from a management perspective like the ISO-2000." (*10KSINTUAE14p2)

> *"…there isn't one set of guidelines but the other thing that would lap onto the successful management of a lab is to have the general business processes assured as well or tested as well, and to do that, the ISO standard come to play. So, ISO*

9001-2008, quality standard. All labs should have that. It is…it's less about the technology, it's more about the processes." (14ETINTUK14p2)

"And we've got also on top of that we've got ISO, so we try and write up, you know, step by step how to use a particular software, how to use a particular data." (16WPINTUK14p21)

The participants, however, are clear that there is no ISO standard for developing and managing a lab that is specific to DF. The closest available standard is for managing forensics labs in general, not specific to DF but also other types of forensics labs. Some participants naturally combined the ISO standard with the American Society of Crime Lab Directors (ASCLD) standards, which is understandably so because the ASCLD international standards simply adopts the ISO standards with additional ASCLD specific standards. Two participants described this combination approach:

"There is a quality management system for running labs. The one we adopted was the, the ISO-17025 standard coupled with the ASCLD, American Society of Crime Laboratory Directors. This basically highlights the quality management system. It comprises of a technical manual, an operation manual, and a coaching manual. So, it's an inclusive process: people and technology." (11CTINTUAE14p1)

"*Yes. We follow two guidelines. The first one are the American interpretation, standard for DFL and we made up our own standard as a framework we use for the…how to…a framework that became inherited from the interpretation, the ISO interpretation for DFL and we made our own framework that gave us all of the process, the workflow and how to handle all these forensic cases."* (12CTINTUAE14p1)

At other end of the spectrum is the participant who holds the positon that has accreditation with ISO, especially under ISO-27001 or ISO-17025, would not be

essential since ISO-9001 on general quality standards are sufficient. This is especially a reasonable position when ISO accreditation is financially burdensome.

"I don't believe you need to be accredited to 27001 or 17025. I think those are good but they're optional. They're a big burden. They are both of them are big financial burdens...And I'm not sure what they achieve over and above ISO-9001. ISO-9001 is a standard that says, we have these standards and processes. It doesn't matter really what those processes are, but they are accredited, which means you are…you obey them, and it's an internationally accepted standard. To be honest you could have a standard that says we've received the evidence, we stick it…we put it in a room. There's 27 people. We don't control the access to it. That's our standard. You get a tick mark. So, standards are all about writing something that passes a tick…So, I don't put in a lot of weight into 17025. I put a lot of weight into 9001." (14ETINTUK14p18)

Overall, the ISO does not provide a standards guideline for developing and managing a DFO or DF facility. The ISO instead acts as a general guideline on quality and forensics labs.

6.2.7.1.3 ACPO Guideline

Some participants referred to the ACPO guidelines, though it is only applicable in the UK. One advantage of the ACPO guidelines is that it addresses specific management issues like training, HR, and processes and procedures using the ACPO principles. Primarily, ACPO is recognised for its guideline for lab managers:

*"Standard guidelines…for digital forensics?...Yes, the ACPO Guidelines… There's also a management guideline produced by ACPO as well." (*05BJINTUK14p1-2)

Again ACPO, The Association of Chief Police Officers have guidelines for managers." (13NXINTUK14p1-2)

*"there are some general guidelines, the ACPO, Association of Chief Police Officers, is guidelines. I can mention a couple or both…the Lab Managers Guidelines and also the Forensic Consultants Guidelines. They are published by ACPO. There's another set of similar guidelines published in the U.S., but in UK we adopt the ACPO Guideline." (*14ETINTUK14p1*)*

Two participants went a step further and identified ACPO as a guideline for setting up capability, especially in terms of response.

"there's guidelines that's related to it, but there aren't specific guidelines. So, in the UK we have something called the ACPO Guidelines and they provide an overview of what is the deal with the digital forensics lab and how to set up capability to respond to different scenarios.... The Association of Chief Police Officers have guidelines for managers." (13NXINTUK14p1-2*)*

*"ACPO's put together a set of guidelines. It's like a lot of book that you can find…you Google it you'll find it. That talks about capabilities of high tech crime, talks about in terms of staffing and what staffing to go on. It talks about what high tech crime units should have in them, what capabilities they should have in them and it's very much a strategic document. It' not in depth… but it is quite good cause it talks about the four principles that we all in law enforcement sort of confine to…" . "(*16WPINTUK14p1*)*

ACPO is perhaps the closest guideline for creating DF capability, even if its application has been limited to law enforcement bodies.

6.2.7.2 Lab accreditation

Participants also discussed the issue of whether labs need or should have accreditation to achieve DF capability. The participants were asked the following question:

*"Do you think laboratory accreditation by ISO or any…any organisation is beneficial?" (*11CTINTUAE14p6*)*

Some participants viewed accreditation is necessary to achieve even though at the very least, a minimum level of quality standard.

*"It is crucial…to follow those standards cause they outline exactly all the necessary steps that's need to be taken when maintaining your devices, when handling cases, to maintain…follow chain of custodies… handling artefacts, building on capabilities of your human resources and analysts…All of those are covered in those standards." (*11CTINTUAE14p6-7*)*

Accreditations for additional types of ISO like ISO 27001 or 17025, however, were seen as unnecessary by some participants such as:

*"…It definitely needs to be accredited. There needs to be some…the minimum accreditation would be quality standard…I don't believe you need to be accredited to 27001 or 17025. I think those are good but they're optional. They're a big burden. They are both of them are big financial burdens." (*14ETINTUK14p18*)*

6.2.7.2.1 Reason for accreditation

Other participants viewed accreditation as "depending on the reason for obtaining accreditation in the first place" which meant they view accreditation according to the type of services they will provide. One participant, for example, stated that accreditation may not be necessary except when need depends on the type of business:

*"I think it is, but I don't think it's required…It's good to have but not a must have. Cause at the end, you know, it all comes down to what sort of business you're doing." (*08SLINTUAE14p10-11*)*

Another participant viewed maintaining the organisation's reputation as the main reason for accreditation:

> "*Beneficial for the name of the organisation. You could be the best one for computer program, for example, however you don't have the degree. No one will see you as a professional programmer. So, yes we have, must have the knowledge and we must have a proof of that knowledge." (12CTINTUAE14p5)*

Still, others simply viewed accreditation as a means of enhancing the quality of the services:

> *"There needs to be some…the minimum accreditation would be quality standard." (*14ETINTUK14p18*)*

> *"I think so, yes because it does show that you're following a standard…and that's the difficulty is showing whether you meet that standard or not." (*15RMINTUK14p29*)*

Other participants use accreditation as a way to create a benchmark for the DFO:

> *"I feel it's a benchmark that should and must be done. It is no harm if you stick to certain accreditation. It gives you a basic benchmark, but each should not be the end of it. Usually organisations become less proactive and they become certified." (*03ALINTUAE14p17*)*

> *"I think it is important but it's important that it's adopted widely. Otherwise, it's just another piece of paper or it's just another accreditation. I think for something to be, to be worthwhile, it has to be accepted, not only by the industry but those who work with that industry. Where it is useful is it, it allows you to set a benchmark. Everyone must meet Level One, for example, if they don't then…it's like the ISO standards. You know what you're getting to an extent if you go to an organisation whose ISO 27001 compliant. You know they have awareness of information*

security. If they don't have that in place, they might have that awareness but you don't know. You've got nothing to objectively assess that, so I think it's important to have but it has to be accepted and recognized." (13NXINTUK14p7)

A concern with making the ISO a benchmark, however, is that the ISO's standards would not be met by smaller organisations. The benchmarking suggested by the participants, therefore, is self-imposed and not one they would necessarily suggest being an industry-wide standard benchmark.

Finally, one participant stated that accreditation may be necessary only because a client may require accreditation from a DFO.

*"accreditation but in general, certifications and everything else, some clients will require you to be accredited or certified or something else for you to even be considered for business at that point." (*09MDINTUAE14p8*)*

6.2.7.2.2 Accreditation Not Necessary

Despite the fact that a majority of participants have accreditation, there are some who do not think accreditation is necessary.

*"…to be honest, I don't think it's necessary. I think, as I was saying before… It's not the practice, it's the people." (*05BJINTUK14p8*)*

*"Well, the goal of the standard is to have efficient, safe environments. And so…you don't really need to be accredited by…you are following these standards. Even if you try to do the best lab, you will be following the standards without knowing it. So having efficient, safe performance lab, yeah, it is very recommended. Accreditation, I don't believe in. So if you follow the standards, I'm not sure you need accreditation." (*10KSINTUAE14p7*)*

Certainly accreditation is not a requirement in the DF industry but something DFO may strive for.

"I think it is, but I don't think it's required." "(08SLINTUAE14p10)

One participant made a distinction between the role of accreditation in private versus the public sector, and that accreditation does not seem to make much sense in the public sector when there is no choice, even with regards to the quality.

> *"I don't think it's beneficial …let's put it this way, if I worked in the private sector I'd say it's useful…But we work in the public sector. Nobody is gonna go anywhere for this but here, so is it good to have, is it good for the forensic community, absolutely. Is it important, probably. Will we get it, yes we're gonna have to do it." (*16WPINTUK14p10*)*

What is perhaps most important, according to one participant, is to follow a standard that is best suited to the needs of the DFO.

> *"It's always good to have ISO standard or ISO certification for your lab but again I would say it is not that best case. It is just to say that you are following international standard but you need to make your own standard based on your own relations, based on your own law and your own case. This would be the best case." (*07COINTUAE14p10*)*

6.2.7.3 Key Success Factors

This subcategory it is characteristically related to the category standards, group concepts that relate to key success factors that DFO identified. The common ground in this subcategory is the concept of quality. DFOs seem to view themselves as successfully based on the level of quality they provide in terms of service, product, and results. As quality is the aim of standards like ISO, it seems appropriate to key success factors under the same category.

Some participants described their key success factor as ensuring quality, which emerged as a general concept of quality, as a result of a set of standards or procedures, or as the proficiency of the investigation process. Overall, the concept of quality seems to share a concern for process and standardising the process in the organisation. One participant explained the concept as follows:

> *"…it is a brand name which has been…become associated with quality, quality services and if you look at the processes, the interview processes that are required to become part of the team…"(*09MDINTUAE14p4*)*

The process that the participant describes covers processes relating to the investigation but also to the way people are recruited. In other words, quality is viewed holistically throughout the entire organisational process, and not only at the laboratory.

Another participant, described quality in terms of the feedback mechanism from customers. It is a function of quality that is beyond the beginning stage but rather stays at the continuous improvement stage of capability. The participant, therefore, explained quality as follows:

> *"We always focus on the quality of our work. We always go back to our customers, constituent and get a quality feedback from them." (*12CTINTUAE14p2)

Some participants credit the standard and procedures as the reason for success through quality. These standard and procedures create a mastery of craft that inevitable leads to quality.

> *"Besides that, it's from the standard, the standard itself has a step by step guidelines on how to implement a digital forensics strategy and also ensure that all the artefacts that you collect are safely handled and securely stored." ."(*11CTINTUAE14p3*)*

*"…I think our processes and our procedures are quite good. We've been doing it a long time so we've got a number of expertise in this field." (*16WPINTUK14p5*)*

*"…I guess control is the ultimate. It's having a well-defined control mechanism because you need to control, not just the evidence." (*14ETINTUK14p8*)*

The quality that the participants describe must also relate to the DF investigation process. In this sense, one participant described quality in reference to proficient investigation analysis together with proper training.

*"The key success factors, first of all, is to have proficient analysis, investigation analysis…that undergo certain trainings to reach acceptable level…after that it's an ongoing training and then it's the efficient of all the tools that we have. So, …we cover all areas." ."(*11CTINTUAE14p3*)*

Quality can also be viewed in terms of the people. As suggested above, quality may come from the process the DFO follows in regards to recruitment. One participant described this as a strict validation of people, or a vetting policy.

*"there is a very strict validation of the people that are…joined the team, to make sure that they can deliver the goods" (*09MDINTUAE14p4*)*

In the end, what matters most are the results and the quality of the results. So one participant simply stated that the key success factor was:

"*…getting some good results I would say*". (15RMINTUK14p9*).*

6.2.8 Organisational Policies

One of the categories of the data that produced a significant variety of concepts is the "organisation policies". Participants discussed numerous policies in place in their organisations whether they were formal or informal. What became clear from the data is the

significant role that organisational policies play, not only in managing the organisation but also in creating a DF lab that is more efficient and producing reliable DF evidence.

This section below highlights the policies which the participants deemed most essential and these policies generally can be grouped into the following subcategories: “information security policy”, “tech use policy”, “confidentiality and non-disclosure policy”, “non-compete policy”, “conflict of interest” and “policy as capability.” The last subcategory is not a type of policy, instead examines statements from the data that emphasize the idea that policy is an essential component of what it means for a DFO to be capable.

The participants were asked whether they had policies in place for governing people in the labs and the organisation:

> *“Do you have any policy to govern your employees in the labs and organisation?.”(*09MDINTUAE14p8*)*

Participants clearly stated the existence of sets of policies in their DFO, but most of these policies were understood by participants to associate to the employees and focused on control of the employees. One participant explained the policy as employee based and not specifically related to forensics:

> *“Yeah. We have specific policies which every employee has to read and sign off on before they actually begin to have access to the labs…Confidentiality? Absolutely…Conflict of interest? I guess that would be not just related to the forensics but in general for the company, I mean.”(*09MDINTUAE14p8*)*

Another participant explained policy as part of following standards like ISO.

> *“…a lot of policies…Must have confidentiality…We have all of that covered by standard, the TOB standard and the ISO standard that we have to follow.” (*12CTINTUAE14p6*)*

Even a DF tool vendor in a very specific type of DFO, has general policies in place that govern technology and people:

> *"Obviously we don't have a lab, but we have general policies in place that govern internet use, etcetera, etcetera. All the standard HR policies." (*13NXINTUK14p7*)*

What becomes apparent from the participants' responses is that there is no standard for implementing policies in a DFO, a standard which identifies the role of policy as a type of capability and in relation to other types of capability like people, infrastructure, and investigation. As such, participants tend to understand policy and its application in DFOs in an ad hoc manner and not as a cohesive and comprehensive type of capability.

6.2.8.1 Physical and Information Security Policy

A DFO's information security policy is one of the key policies in an organisation, and concepts that emerged and related to this subcategory are "access control and accountability", "isolated internal network", "no wireless connectivity", and a "need to know basis policy." These concepts contribute to create an initial impression of what an information security policy may comprise of.

One important type of policy to secure information relates to controlling access to the DF lab and creating accountability for that access. Access control must be a process in the DF lab and also a policy for the DFO that includes documentation. One participant described this policy, process, and procedure as follows:

> *"…only authorised people should get access to the, to the premises, for example, if there is an evidence room, lockers different things, then only authorised people should get access to that facility. There should be kind of log or record where we read, we write down who did what, at what time, at what date. So it's like kind of audit trail…kind of log of activities…just to follow up and if there is something wrong to know who's person will be held accountable for that action. Yeah, this is for the access control as well."* (04AUINTUAE14p1)

One participant described this access control as an essential part of policy and policy as an essential capability for a DFO:

> *"They're important not only to capability but also to control what's going on in your organisation. And if you don't have policies in place, then potentially people will…they don't know where their boundaries lies so they can steal data and they're not to be held accountable, for example, so you need policies in place to control your environment and control what people can and can't do."* (13NXINTUK14p7*)*

Another participant described access control as part of a layer of processes that create a successful forensic process, stating that access control, which among others, on its own is insufficient with a peer review policy and process.

> *"For example, we can receive some evidence, store that evidence appropriately and control its access to it appropriately and we can perform forensic analysis to that data and we can produce a report and that report can be accepted by prosecution or defense. That's not necessarily a successful forensic process. What we have to do is have a process of peer review built into it" (*14ETINTUK14p5*).*

This participant is essentially describing a holistic view of policy as capability. One cannot look at a policy on access control, therefore, in isolation from other policies.

One participant added that a policy regarding technology use must include isolating the network, use of certain types of technology, and storage of large data on the network. Overall, the participant raised the issue of an isolated internal network:

> *"..there are several policies which go from now, from not having the mobile to how to control the taking of picture, how to control large storing evidence" (*03ALINTUAE14*p20)*

The isolated network must also be accompanied by a no wireless connectivity policy within the DFO. In other words, there is a distinction between internal and external policies, including the presence of technology inside the DFO or the DF lab:

> *"I said the most important one in the current is no wireless communication, no internet access in the lab where you're doing work, apart from one machine that*

*you can use for research that is not connected to the network you might be using in the lab." (*05BJINTUK14p10*)*

*"So, internally, our policy is different. How we are managing that, stopping taking pictures of the code…and mobile USB, internet connectivity…all sorts of thing…BYOD type of thing, bring your own device type of thing…" (*03ALINTUAE14p19*)*

Aside from the restrictions on technology and access, a third layer that a participant identified is a "need to know" policy at the management level.

*"Need to know basis even though it's law enforcement, but you know you cannot go open…okay this case is open, everybody is invited, have a look. No, it…this…it cannot happen." (*03ALINTUAE14p19*)*

Such a policy goes beyond confidentiality as it limits the spread of certain information throughout the DFO.

6.2.8.2 Tech Use Policy

A policy that relates directly with information security is the "tech use policy", sometimes referred to an "acceptable use" policy.

*"Acceptable use policy. Certainly." (*09MDINTUAE14p9*)*

The "tech use policy", however, covers in detail the use of specific types of technology such as internet and wireless connectivity, mobile phone use, email and password use, screen copy/past, backup/maintenance, and cloud use, among others. These policies can relate to quality standards as well, as explained by the following participant:

*"Yes we do….We have two processes. It starts with the contract among the staff…So contract of employment with the staff has an appropriate use document that goes with it and an IT security document that goes with it, and that's all part of our quality system." (*14ETINTUK14p19*)*

6.2.8.2.1 Internet/Wireless Use

Participants described various features of an internet/wireless use policy. The primary feature is the prohibition on wireless connections inside the DF lab.

> *"We don't use wireless connections for any purpose. It's all hard wired." (*05BJINTUK14p9*)*

> *"…in the department we only had one machine that was connected to the internet and that, and that was …Oh definitely, yeah, it wasn't attached to our network at all. There was no internet connection on our lab network. We had a separate room with a separate computer, so if the case involves going to look at some websites to see what they were, then you go into that one and you do that there…" (*15RMINTUK14p34*)*

> *"Yes. We follow the ISNS, for internet for computer using, for how to access it, how…you must have antivirus, you must have …all, we have all the policies. There's a lot of policies." (*12CTINTUAE14p7*)*

This policy can also be enhanced with an internet usage policy by the DFO. The rest of the DFO not within the DF lab could have a different policy.

> *"So the corporate environment, we've got internet, but we restrict it, we monitor it. We don't allow outbound POP or SMTP…" (*14ETINTUK14p21*)*

> *"Exactly. Internet usage policies..." (*11CTINTUAE14p8*)*

6.2.8.2.2 Mobile Phone Use

Another policy governs the use of mobile phones, especially smartphones. Participants were asked the following question:

> *"Do you guys have policy in place in your organisation which governs the use of mobile phones…" (*10KSINTUAE14p8*)*

> Three participants stated that they had such a policy:

> *"Yes." (*14ETINTUK14p19*)*

*"yeah we have the usage guidelines for mobile phone within the company…" (*08SLINTUAE14p11*)*

*"Yes, yeah, yeah. Actually, our products do include the control of all devices and the Russians are really strict about that. And they control, I mean we have like our own mobile phone devices has a solution, you know, of the single process. And it's part of our enterprise rules now." (*10KSINTUAE14p8*)*

There was one participant, however, who indicated the lack of a mobile use policy:

"Using my own phone?...Not that I'm aware of. No, no…" (16WPINTUK14p11*)*

The data shows that while a mobile phone use policy exists in some DFOs, the policy is not applied throughout in the industry.

6.2.8.2.3 Email & Password Policy

A participant also raised the concept of email and password policy when discussing the types of policy present in the DFO.

*"Email policies, passwords and so on." (*11CTINTUAE14p8*)*

An email and password policy can be important for a DFO to prevent security breaches through malware embedded in email links, and to avoid hacking of passwords. A USB or Flash Drive Use policy is similarly important because of security concerns. Such devices could become potential sources of viruses or malware:

6.2.8.2.4 Screen Copy/Paste Policy

Another policy that falls under the tech use subcategory is the screen copy/past policy, which aims at preventing unauthorised duplication of the DFO's data.

"I mean, how many law enforcement agencies are applying a policy where they're restricting a screen copy, paste policy. Do you know about this policy? Restriction on the PC of the evidence, so that the screen button on the keyboard…to make a screen capture is disabled…" (03ALINTUAE14p20)

The participant implies, however, that this policy might not be common in the industry, especially in the law enforcement context.

6.2.8.2.5 Backup and Maintenance Policy

A DFO should also have a backup and maintenance policy as part of securing its data.

> *"…including internet, including servers, or work stations…and…policies to also help users like ahm…backup policies…like ah…maintenance policies and so on." (*07COINTUAE14p11*)*

6.2.8.2.6 No Cloud Use

Finally, a tech use policy must address the issue of cloud computing discussed above. Cloud, however, poses issues of security. As a response, a DFO may add a no cloud use policy. So when asked about the use of cloud, the following participants responded as follows:

> *"no … that would be one of the things that we definitely do not, so again, that's our policy" (*09MDINTUAE14p7*)*

6.2.8.3 Confidentiality & Non-Disclosure

Almost all participants indicated the existence of a basic confidentiality and non-disclosure policy. Such a policy is standard in the industry and in other industries as well. As such, it is treated as part of an employment agreement:

> *"…it is anyway because as part and parcel of the job, you've got to sign the office secrets which means you've…you know, you've already got that layer of confidentiality there, you know. They knew that they weren't allowed to discuss things outside and so on…" (*15RMINTUK14p31*)*

> *" Yes. We have ah…a regulation in place and we all sign it when we join… so it is mainly some part of it is about confident, confidentiality of the information, our client or our investigations." (*07COINTUAE14p10-11*)*

*"confidentiality? Absolutely. Again, that is, by confidentiality of the job we do…" (*09MDINTUAE14p8*)*

*"Yes. Must. Must have confidentiality." (*12CTINTUAE14p6*)*

*"…in that terms, no they just follow the general guideline of the company…On the backend, our employees already signed an NDA with the company itself." (*08SLINTUAE14p11*)*

Additionally, a non-disclosure agreement could be entered between the DFO and the client in addition to the one between the employee and the DFO.

*"…on the first point, before we do an investigation, first we have a final NDA with the customer…a non-disclosure agreement…that will lead quickly to confidentiality agreement. So that's the first step we do before we start any work with the customer. That's the first document that needs to be signed, okay? On the backend, our employees already signed an NDA with the company itself. Okay? So, just to secure that one." (*08SLINTUAE14p12*)*

*"…we have nondisclosure agreement and confidentiality agreement for employees and our client to maintain the information." (*10KSINTUAE14p8*)*

6.2.8.4 Non-compete

Another policy that is normally included in the employment contract to prevent piracy of talent is a non-compete agreement. This policy, however, can also act as a means of information security policy, as explained by the following participant:

"It's in my contract that I cannot go up to any other company that are competing with or working at the same field and this is again to protect the client not to protect even …because, let's say, I am now interacting with some clients that is high profile client or highly confidential client and then I leave my company so all the restrictions are away. So, I have in my contract fair freeze that I have to keep the

*confidentiality of the client and I cannot work with the competitor." (*07COINTUAE14p11*)*

6.2. 8.5 Conflict of Interest

Finally, participants indicated that a conflict of interest policy exists in DFOs. The purpose of such a policy is to deter third party influence or any other influence on a DF staff due to the conflict of interest:

*"Conflict of interest? I guess that would be not just related to the forensics but in general for the company, I mean." (*09MDINTUAE14p8*)*

6.2.9 Knowledge and Background

Participants were asked about the knowledge or background necessary for a person to become a digital forensic investigator, perhaps at the key position in the DFO.

"*…what do we need to become a digital forensic investigator? Do I need a specific qualification to become?*" *(*07COINTUAE14p15*)*

The findings in the data shows that concepts that fell under the category "Knowledge and Background" produced a set of knowledge and background that can be divided into the following subcategories: "IT", "Security", "General Forensics", "Specialized Skill", "Operating System" and "Programming".

Participants' replies seem to suggest that there is no single formula that will lead to a good DF investigator, citing the diverse backgrounds of participants. Perhaps a combination of a set of knowledge and background in IT and Security may be as best as suggested by the following participant:

*"I would say very good plus to have a good background on IT. Also another good plus if you have background on security. And then you need to study to understand the technologies, the solutions and so on." (*07COINTUAE14p15*)*

6.2.9.1 IT

Participants seem to agree with the necessity of having a background in information technology.

*"It does matter. The forensics analyst must be IT literate…." (*11CTINTUAE14p9*)*

One participant, however, seemed to view the IT background as something that can be taught or learned on the job, allowing one to teach an investigator about IT.

*"…yes you need technical skills in relation to computers, most definitely…but either way you could take if you like somebody who's got a degree in IT and teach them how to investigate. Or you can take an investigator and teach them about IT." (*15RMINTUK14p39*)*

One participant even said that anybody can be trained as long as the person has a technical background.

*"So, is the user trained to use that or has, if appropriate, qualifications and skills to do that particular task. You can use anybody. We've got a guy here, Rob. He's not a forensic technician, but he is an IT technician." (*14ETINTUK14p9*)*

6.2.9.2 Security

Yet, some participants insisted that a background in security is also important to have for a DF investigator:

*"it must be related to computers and somehow to security." (*12CTINTUAE14p9*)*

"…also another good plus if you have background on security." (07COINTUAE14p15)

"*No, he must have a security background." (*08SLINTUAE14p16*)*

6.2.9.3 General Forensic

Other participants saw that background ought to be a combination of both IT and security with an ability to understand the general forensics process:

*"…the information, or at least the knowledge on all basic, all the fundamentals of forensic security…on how people, how to secure applications, how to hack systems, how to do assessments and all that of course will happen to become a better analyst…" (*11CTINTUAE14p9*)*

*"Just like going on an Encase course. It doesn't mean, make you a good forensic analyst. It just means you can use Encase…I think the combination is the first thing you need is the ability, is the instinct to be able to understand what the data is doing. The computer architecture, understanding the data structures. So, I would be very happy taking somebody who doesn't understand investigations, doesn't understand forensics but understands how to string a pattern, make their own computer, how to build their own computer, how to work in Linux. I would take those in a heartbeat cause those are the people that you can teach the process of forensics and the process of investigation." (*14ETINTUK14p27*)*

6.2.9.4 Specialized Skill

Another way of looking at the necessary technical and educational background of the people in the field is to consider where DF as an industry is heading. Some participants are looking at specific skill sets or a specialisation in the DF field that could prove valuable, or even a combination of specific skill sets are needed.

*"I think perhaps the best answer is you're looking for a range of experience. You can go specialist and you can be really deeply specialized in one area and that would make you a really good forensic analyst." (*14ETINTUK14p28*)*

*"Well it depends, you know, the forensic domain is becoming quite big so you have specialty. Some people are specialized in reversing tools, for example, and they should have the government experience. Some people have, for example, leading the investigation and collecting all sorts of evidences and then correlating feeds in a real world scenario, some people are focused more on small things and how the technology could work to block network attacks or how attackers can bypass technology. And you need a bit of all of these are specialties." (*10KSINTUAE14p11)

Other participants identified knowledge of operating systems and programming as specialized skills that would be necessary for a DF investigator.

*"…He must have a good knowledge on operating systems. And ah…he should be able to use all the tools for investigations." (*11CTINTUAE14p9*)*

*"…you need investigators with varying levels of experience and different backgrounds. So that could be a Linux expert, a Windows expert, a mobile expert, for example, with different levels of experience…" (*13NXINTUK14p8*)*

"Personally, I like someone who know how to write a program, a software engineer a bit like me…Because I think you understand how the machine works under the bonnet. And I think you can make an assumption about something that other people can't because you know how a processor works. And you say well it has to be this way because that's how the computer would do it, you know. It can't be that way because that would go against programming techniques. It would be a really

*strange thing happening. So, I think it helps. It's not an essential but I think it definitely helps." (*15RMINTUK14p40*)*

6.2.10 Education

The category of "Education" encompassed concepts from the participants' interviews that related to the participants' educational background. While participants discussed some of these concepts in the context of their background before joining the DF field, some participants also talked about the benefits of having an education related to the field while some discussed the necessity of an educational background related to DF investigation. This section discusses the concepts that arose from participants' interview data and this could be grouped into three subcategories: "type of discipline", "level of degree", and "necessity".

Participants came from various disciplines, and there was no discipline that stood out. In other words the DF industry has not yet created a standard on what type of education and training is needed before working in DF. The following academic disciplines emerged from the data:

Degree	Data
Computer Science	"So, I did a computer science degree…" *(*05BJINTUK14p17*)*
Software Engineering	"Personally, I like someone who know how to write a program, a software engineer a bit like me." *(*15RMINTUK14p40*)*
Computer Forensics	"I've got Master's degree in computer forensics." *(*16WPINTUK14p18*)*
Digital Forensics	"I have a degree in digital forensics…" *(*13NXINTUK14p1*)*
Information Security	"Well I have a Master, Professional Master in Information Security… I am currently taking a PhD with Brunel University London in Information Security…" *(*10KSINTUAE14p1, 10*)*

Table 16 Academic Disciplines Emerged from the Data

While there is no requirement in the industry as to the level of the degree, one participant noted an experience where a higher level degree, such as a Master degree proved helpful with regards to qualifications as an expert witness, an advantage that the participant suspected over those that did not have a higher level degree:

> *"Because of my MSC and my degree and, you know, when I'm writing my statement I'm putting…I've got Master's Degree in computer forensics. So it makes it very…for some reason and it's probably because of where the legal system is in the*

*UK and their understanding of computing and forensics in those diver…they don't seem to question that. They don't question it as much. Now, there's some really good bright people in there who are a lot clever than me I can tell you that for sure who are constantly called to court" (*16WPINTUK14p18*).*

The necessity of a degree, according to participants is not due to some specific knowledge gained from the degree, rather as a starting point for show aptitude.

"I would tell you any degree. I don't care what your degree is in as long as it's a hard sub…soft degree like humanities probably not. But a science degree, mathematics, physics, biology, chemistry…technology, any kind of technology. Anything…a good quality degree is a first starting point. The only reason for that is that it shows the ability to learn and to research and to apply yourself to your process. So I don't really mind what your degree is."(14ETINTUK14p30*)*

Instead of solely relying on a degree, one participant highlighted the need to balance between academic qualification and experience:

*"…it's hard to balance actually because in a lot of industry you need a degree or some kind of academic verification. Traditionally, the forensic industry has been very, very focused on experience…experience driven …but now there is a lot more academia, so I think academia is essential. But I don't think it's the overall solution because without experience it…you…apply the knowledge that in the academia is really tricky. And I can say that from experience. I had a lot of graduates who were very, very smart people but they don't understand how to articulate and to relay what they've learned in their degree, you know, in a real life environment. So, I think you need both." (*13NXINTUK14p9*)*

Experience is discussed in the next section, which is closely related to academia when determining qualification.

6.2.11 Experience

The category of "Experience" encompassed concepts from the participants' interviews that related to their work experience which helped them in the DF field, and also to the participants' opinion on what formal or informal experience they value for a career in DF investigation. The participants' responses created data on various concepts that can be grouped into the following four types of experiences named as subcategories: these include "industry experience", "law enforcement", "software development", and "computer security". Additionally, the concepts in the data revealed the participants' views on how the experience may be acquired and on the length of the experience.

One participant explained that the DF industry is experience driven, highlighting the need for DF investigators to additionally gain experience rather than just academic background:

> *"…traditionally the forensic industry has been very, very focused on experience…experience driven and…but now there is a lot more academia, so I think academia is essential. But I don't think it's the overall solution because without experience, applying the knowledge that in the academia is really tricky. And I can say that from experience. I had a lot of graduates who were very smart people but they don't understand how to articulate and to relay what they've learned in their degree, you know, in a real life environment. So, I think you need both" (*13NXINTUK14p8*).*

As far as the length of industry experience, the participant indicted that a minimum of two years are necessary but that there may not be capping on experience:

> *"they need to be doing the job for at least two years, I think. Just to give them enough awareness to be able to do an investigation independently, but I don't think there's ever a bar where you can say, I am fully capable and qualified investigator*." *(*13NXINTUK14p9*)*

Another participant agreed with the two years minimum:

> "*From my experience, I see that requires a minimum of two years to become a certified digital forensics analyst who can work alone and do cases by himself."(*11CTINTUAE14p10)

Although, other participants would require less, showing the lack of and need for a standard set by the industry:

> *"So at minimum it's not less than three months "(*08SLINTUAE14p17*)*

> *"How long experience do I need to become forensic investigator from your point of view? I would say one year" (*07COINTUAE14p16)

Investigator in the field of DF could require more than two years' experience in order to be able deal with incidents or handle cases :

> *"a subject matter expert and capable, I'd say…something five, five ten years"* (09MDINTUAE14p13*);*

Aside from industrial experience, participants also noted their experiences were coming from law enforcement, software development, or computer security.

> *"I was completely self-taught as far as computers was concerned for my first, my first ten years…then I thought, it might be a good idea to get a qualification of some description. So, I did a computer science degree with the Open University. So, I got a full time job as a policeman" (*05BJINTUK14p17*)*

> *"My background was into support. I was heavily exposed to software development. See, knowledge of software development is very, very important." (*03ALINTUAE14p28*)*

"the information, or at least the knowledge on all basic, all the fundamentals of forensic security…"(11CTINTUAE14p9*)*

6.2.12 Training and Development

The category "Training and Development" also encompassed many concepts regarding the training the participants had engaged in and what they viewed as training that would be most beneficial for DF investigators. Participants also stated their position, which seemed to be unanimously held among participants, on the necessity of training, stated that

"*Training is a must.*" (13NXINTUK14, p. 9)

"Yes. It's something we insist on." (14ETINTUK14p30)

"Training is mandatory" (09MDINTUAE14p12)

*"Training is a must…keeping fresh…" (*13NXINTUK14p9*)*

*"And if we don't give them the training they require to do that, then we are morally in big trouble" (*16WPINTUK14p20*)*

Also, there is no standard in the field on what type of training is necessary and how long for or how often. This view was expressed very well in interview 13NXINTUK14, page 10, where the participants stated:

"…so there's certainly qualification out there of value, but I don't think there's a qualification out there that's actually ticks the box and says that, that chap over there is a forensic investigator. He is to a standard, and I think that's what's missing in the industry. And it's something that's being looked at a number of times over the years and to bring in some kind of accreditation. If you go in the building

industry or the law industry, they're accredited and reassessed every couple of years such as charts and surveys, for example. We don't have that in forensics. And I do think there's a need but it's a very difficult thing to achieve, I think." (13NXINTUK14, p10)

However, it also became apparent from the data that participants have different concepts on what the training would be. These concepts, as expressed by the participants, were grouped into the following subcategories: "types of training", "frequency", "training certification as qualification", and "self-education".

6.2.12.1 Types of Training

Concepts emerged from the data relating to the different types of training that people in the DF field undertake or should undertake. These concepts were grouped into the subcategory "types of training."

One participant described training in DF that is based on needs and process, instead of a vendor specific training who trains individuals on the use of specific DF forensics analysis software. One of the leading providers of this type of needs and process based training is SANS Institute:

"I took most of my forensics training from SANS. I would say it was very good for me to take this training. I'm certified as forensic analyst and forensic examiner from SANS. And also incident handler from SANS. What I like about this, this type of training…it's not vendor specific training."(07COINTUAE14p15*)*

"I'm certified as forensic analyst and forensic examiner from SANS. And also incident handler from SANS." 07COINTUAE14p15*)*

*"Well, I know SANS they have…they are advanced malware analysis and forensics. I do believe it is a powerful tool to teach" (*10KSINTUAE14p11*)*

SANS also provides a generalized forensics training that looks at the forensics process instead of just the tools used in the process:

> *"I did a generic forensics training in SANS" (*11CTINTUAE14p9)

One participant noted the need to improve first responders training as well:

> "*First responder training needs to be improved" (*13NXINTUK14p12*)*

On the other side of the spectrum, of course, are tool based training or vendor specific training that is common in the DF industry. One participant stated:

> "*I had to undergo, of course, trainings. So I did, I did the tools training*" *(*11CTINTUAE14p9)

> *"So, things like Encase, NCstink, or a Xways course or an FTK course*"(14ETINTUK14p27*)*

> *"you must have attended a course about forensics…you know, from accredited place call…for example, from a vendor like Guidance, for example… …FTK does some courses as well I believe"(* 08SLINTUAE14p15*)*

There is a downside to tool specific training, however, as noted by the following participant:

> *"So he's not telling you the process, he's not telling you other considerations. So…and this is what I like about training. You should put things in perspective. I don't want to take training about how to use this tool, but I want to understand what is the process and why did I need to use it…" (*07COINTUAE14p15*)*

Some participants recommend a combination of tool and process based training as the optimum type of training:

> *"…beside tools…specific tools training…I recommend you use…go to SANDS training…" (*11CTINTUAE14p10*)*

> *"I had to undergo, of course, trainings. So I did, I did the tools training. I did a generic forensics training in SANS"(*11CTINTUAE14p9*)*

Other participants equated training with keeping up with the fast evolving pace of technology. These participants see training as a way to maintain competency in the field.

> *"Because cases are evolving and technology and cases are evolving so there are new ways to…new hacking techniques, there's a new trend landscape deep…We've seen cases have evolved on PCs to mobiles, from phishing to USB sticks…data linkage with all different mechanisms. So, the analyst must up to date and know about all these things. So if you can add…when walking on a case, identify those new patterns, new anomalies…" (*11CTINTUAE14p11*)*

One issue raised associated with subcategory "types of training" is the purpose of the training. This is an issue that relates directly to the decision on what tools, like forensics analysis software, a DFO should have as part of its capability. A DFO must determine whether a tool-based training provided by software vendor is sufficient to create the minimally required capability. The subcategory also relates to the investigation process as either a process driven or tools driven, or whether the DF investigators are tool dependent or independent. Then, of course, the subcategory relates to policy because a DFO's training and development policy should indicate the types of training that the DFO values for its staff and whether the purpose of such training is to establish qualification, to maintain competency, or both.

6.2.12.2 Frequency

Another subcategory that lends itself to a specific dimension is "frequency" of training. There does not seem to be an industry standard on even such a very basic requirement. Still, the trend in the data seems to show a minimum of two trainings per year are required.

> *"So we always have training…twice, three times a year."* (12CTINTUAE14p9)

> *"Well, hopefully, two courses a year"* (05BJINTUK14p19)

> *"It's very advisable that…be more often. Like as much as he can because it depends on his work. But I would say not less than two time boot camp style to collect information, knowledge required about the technology updates." (*07COINTUAE14p16)

Some participants, however, would leave this to the discretion to the participants and the needs of the participant, and not impose a minimum number of training:

> "*He needs to go for training on these because the approach to doing the investigation will change. But other than that, you know, it's all, it's all the same procedure so it doesn't make sense to do or go through that training again and again." (*08SLINTUAE14p18*)*

> "*I think that differs on an individual basis. Some people like myself have a real passion, so when I go, I do a lot of research myself so I don't necessarily need as much training as someone who may just focus very much on the role. And training means a lot more to them. So, it depends on the person, I think. Sometimes people benefit from a training environment, others benefit from research and development themselves, I think." (*13NXINTUK14p9*)*

Other participants see training as a continuous process, and mandatory for DF staff:

*"It's, it's continuous, continuous thing," (*09MDINTUAE14p12*)*

"Well, continuous training is almost mandatory because ah…you will see, you will see a lot of the knowledge does not come" (10KSINTUAE14p11)

6.2.12.3 Training Certification as Qualification

Some DF analysts seem to equate training with creating qualifications that would bolster one's credentials in the DF field through training certifications.

"*there are obviously the recognized qualifications which are good to have.* "(14ETINTUK14p27)

"Well, it was a requirement they needed to fulfil and my start as a forensic investigator but based on trial…on company trainings. I attended couple of trainings for like XYZ for Encase to do forensics. We do the advance course for that as well so we doing advance forensic, you know, on mobiles and so on and afterwards I had an internal enablement on forensic processes, procedures and so on…by the director" (08SLINTUAE14p15)

There are certainly those people in the industry that deem training as sufficient for qualification:

*"As long as I am satisfied that he's received training and understands the implications of his actions, that's a tick in the box" (*14ETINTUK14p9*)*

One participant, however, pointed out the drawback of relying too much on certification to determine qualification.

"The certifications I think are valuable but the danger with certification is they just certify you using a tool. They don't actually certify you as an investigator. So

*there's certainly qualification out there of value, but I don't think there's a qualification out there that's actually ticks the box and says that, that chap over there is a forensic investigator. He is to a standard, and I think that's what's missing in the industry. And it's something that's being looked at a number of times over the years and to bring in some kind of accreditation. If you go in the building industry or the law industry, they're accredited and reassessed every couple of years such as charts and surveys, for example. We don't have that in forensics. And I do think there's a need but it's a very difficult thing to achieve" (*13NXINTUK14p9*)*

Certification as qualification is certainly questionable when it comes to tool based or vendor training certifications, as explained by one participant:

*"…the danger with certification is they just certify you using a tool. They don't actually certify you as an investigator" (*13NXINTUK14p10*)*

6.2.12.4 Self-Education

Aside from training, participants suggested that DF staff must have the personal motivation for growth and that a DFO should encourage skills and knowledge development to their staff through appropriate policies. In other words, development can be views as a personal journey of self-education, instead of a qualification requirement.

*"So for me it was an experience. So I wanted to be a programmer for a very long time. And then I found out about digital forensics and that's what made me feel that there's a pass for me" (*16WPINTUK14p17*)*

One participant emphasized the need for DF staff to do their own research in addition to the training so there is continuous educational growth:

*"And do their own research and, and teach themselves new areas that somebody else might not have even covered. Ah…for instance, if we ah…I don't know…if a new operating system arrives" (*05BJINTUK14p20*)*

Some participants even created a policy similar to the Google model of requiring employees to have a free time for experimentation and play:

*"But the important thing is the third element here. They should also be given time to play" (*05BJINTUK14p20*)*

*"Twenty percent of their time had to be on research cause that way we learn new stuff. They can develop new techniques. They can play and break things in a non-dangerous way." (*14ETINTUK14p24*)*

The many subcategories of training and development interrelate on multiple concepts and to other categories like tools, people, and policy. Training, therefore, as part of a DFO capability is not an isolated concept. It relates to entirety to the DFO and affects decision making on the types and number of tools available, the number and qualification of DF staff, and policies on training, tools, and qualification.

6.2.13 Organisational hierarchy

The researcher also asked the participants about the hierarchy in their DFO, a question that was aimed at determining the key or various positions in the organisation. The participants' responses led to concepts that can be grouped into four subcategories. The first three subcategories grouped the concepts according to the type of position or function in the organisation: "executive", "technical", and "administrative". The fourth subcategory grouped concepts that considered the subcategory of "type of organisation" as having an impact on the organisational hierarchy. Table below clarifies them more adequately.

Executive	Technical	Administrative	Organization
High level manager (13NXINTUK14p8)	Head of Technical (07COINTUAE14p14)	Admin Staff	Individualized (05BJINTUK14p3)
Board of Directors (07COINTUAE14p14)	Lab Director (11CTINTUAE14p2) (11CTINTUAE14p8)	Administrative (07COINTUAE14p12)	Corporate Consultants/Freelancer (05BJINTUK14p3, 11)
Managing Director (07COINTUAE14p14)	DF Investigators (08SLINTUAE14p14)	Secretary (07COINTUAE14p14)	Academic 04AUINTUAE14p4)
Executive Lab Managers (08SLINTUAE14p14) (14ETINTUK14p24)	Consultant (09MDINTUAE14p10)	Accounting (07COINTUAE14p14)	Vendors 04AUINTUAE14p4)
Head of Forensic Investigation (16WPINTUK14p14)	DF Analyst (11CTINTUAE14p2) (11CTINTUAE14p8) (14ETINTUK14p24)	Service (07COINTUAE14p14)	Law enforcement 04AUINTUAE14p4)
Director of Intelligence (16WPINTUK14p14)	Security Analyst (11CTINTUAE14p2)		
Director of Strategic planning (08SLINTUAE14p14)	Technicians (13NXINTUK14p8)		
Quality Manager (11CTINTUAE14p2) (11CTINTUAE14p8)	Specialist 13NXINTUK14p8)		

Health and Safety Manager (11CTINTUAE14p2) (11CTINTUAE14p8)	DF Researcher High Tech Officer (16WPINTUK14p14)		
Line Manager (12CTINTUAE14p8)	High Tech Assistant (16WPINTUK14p14)		

Table 17 Job Titles Emerged in the Data

Table 18 shows the diverse means in which DFO create the organisational hierarchy. The positions in the executive and technical subcategories do not show a pattern or standard in the industry. Such lack of standard shows that there may perhaps require a potential for improving the DFO structure by creating specific key positions with a standardized position title that can be used uniformly throughout industries with standardized job descriptions and qualifications.

6.2.14 Investigator Characteristics

The participants' interviews also gave rich data on concepts that were grouped together under the category "Investigator Characteristics." The participants, in the process of explaining what they view as essential qualities of a DF investigator, raised concepts that were grouped together into the following subcategories: "investigative", "communicative", "technical", "analytical", "motivated", "and "security clearance." It's difficult to determine which one of these qualities is more important than the other. As one participant put it,

*"It's a combination: ability, experience, education" (*16WPINTUK14p17*).*

6.2.14.1 Investigative

In the subcategory "Investigative", the participants described the DF investigator as having the ability to think like a criminal, to troubleshoot, or be a good detective: presented by few participants stated:

*"Exactly. Yeah. Criminal mind, you know." (*08SLINTUAE14p6*)*

> *"Criminal minds into the metadata…see how things were done."(* 11CTINTUAE14p4*)*

Another way of saying this: is to have to ability to dig deep and troubleshoot:

> *"forensics analysts they have, they have a different mindset. They must, they must have that different characteristics, they must be like, they must be curious, they must know how to dig deep into the metadata" (*11CTINTUAE14p4*)*

> *"he must have that skill. So, unless he had that set of skills, doing that analytical thinking and basically the troubleshooting approach what we call it. So, it applies here as well."* (08SLINTUAE14p6*)*

> *"…in forensics you must find someone with analytical approach. He needs to know how to think, to solve the case, what would have happened. He needs to have everything, to link different things together, to identify an event…"* (08SLINTUAE14p6*)*

Another participant described it as a "frame of mind":

> *"It's a frame set. It's a state of mind" (*03ALINTUAE14p28)

One participant also pointed out that it is easier to teach someone with the right frame of mind as to what is investigation rather than to teach a technical person how to investigate:

> *"We've found it is easier to teach serving detectives how to examine computers than it is to say in fact…or go to people with doctorates in computer science to turn them around and be an detectives"* (05BJINTUK14p18*)*

6.2.14.2 Technical

Other participants viewed the technical ability of the DF investigator as the primary trait above all else.

> *"So, for me the first thing is technical ability, technical aptitude"* (14ETINTUK14p28*)*

> *"So I would rather find somebody who's a really good hobbyist IT person who understands the technology first and then teach them the process."*(14ETINTUK14p12*)*

One participant even went as far as saying that a DF investigator should have a software engineering or programming skill to become an effective investigator:

> *"I would see him with mainly two things. Does he have the software engineering knowledge? Does he have the programming knowledge? Because these things matter" (*03ALINTUAE14p5*)*

The key is for the DF investigator to be technical enough and not be too dependent on the tools.

> *"The real challenge is somehow inspiring them to be independent than the tools"* (03ALINTUAE14p11*)*

The dependency on the tool is a concern that was raised early in this chapter in the discussion section about tools and tool selection. In other words, the ability of a DF investigator directly impacts the requirements for tool or technology capability. It is the person who uses the tools, after all, to conduct the investigation and not the other way around.

6.2.14.3 Analytical

A DF investigator must also be analytical, according to some participant.

> *"So he has to start at some point…he must have that skill. So unless he had that set of skills, doing that analytical thinking" (*08SLINTUAE14p6*)*

The type of analytical skill also varies for participants. One related the analytical trait to the ability to be creative while another related the analytical skill to being holistic, or seeing the problem in its entirety.

> "*Definitely. To be intuitively to be creative in your work."* (12CTINTUAE14p9)

> "*and look at the whole thing holistically at the case"*(11CTINTUAE14*p4)*

6.2.14.4 Motivated

One participant was optimistic about the ability of DF investigators, and singled out motivation as the sole factor necessary to be a good DF investigator:

> *"Well you need motivation. That's the only thing you need…most of the things that you learn in this domain are things you learn on personal effort"* (10KSINTUAE14p10*)*

6.2.14.5 Security Clearance

Finally, a DF investigator, minimally, should meet security clearance checks and background checks.

> *"And for us, in my lab everyone has to have the ability to go through security clearances and get the appropriate security clearances. They have to be vetted"* (14ETINTUK14p12*)*

In the end, what really matters, it seems, for a DF investigator is to succeed the desire to establish the truth by establishing what happened:

> "*The key success factor is trying to establish what happened. Trying to establish the truth." (*05BJINTUK14p3*)*

6.3 Identified Core Categories of Digital Forensics Capability

After identifying the categories and subcategories in the previous section based on the grouping of concepts and phenomena and after thorough analyses of the relationships of these categories and subcategories taking into account their significant dimensions, the next task under the selective coding process was a higher level and more abstract form of identifying relationship and categorisation. What emerged from this process is the researcher's identification of the four core categories: investigation, infrastructure, policies, and people.

It should be noted that these four core categories also appeared in the codes from the participants' responses. For example, as you may recall from the "Capability" category, the participant in interview 07COINTUAE14 stated as follows:

> *"Okay, so they must have …policies and procedures implemented…um…people must know how to handle cases and there must be a chain of custody kept…so they must be pre …prepared for that. They must know exactly what digital evidence received, how they handle this and must be a process already in place. So…ah…chain of custody…um…people who are aware of the technology and ah…how to use it. And then…ah…maybe HR rules and legal rules of how they will handle these investigations."* (07COINTUAE14, p.6)

The participant essentially identified all the core categories with the following concepts: "investigations", "technology", "policies and procedures", and "people". Other participants also usually identified three of the four categories. What differs, however, is the depth to which the participants understood, linked, and discussed these categories.

This section, therefore, aims to give a preliminary explanation of each of the four core categories, and the categories that gravitated towards being grouped under the relevant core category.

6.3.1 Investigation

The core category of “Investigation” should be understood as the interaction of three sub-categories, the findings of which were discussed in the previous section. The three sub-categories that naturally group under the title of investigation are “Investigation Process”, “Investigation Procedure” and “Evidence Admissibility”. This core category encompasses a set of phenomena that occur towards the end of the DFO’s procedural lifecycle. It is where they focus on the output, hence, digital evidence.

The research views this group of categories as a core set of capability that is distinct from the other core categories. In other words, the category Investigation requires a unique core capability that includes the investigation process, a set of procedures surrounding the investigation process, and capability that increases the likelihood of producing admissible evidence.

6.3.2 Infrastructure

The core category of “Infrastructure” is not solely limited to the physical infrastructure, but also the building of the laboratory to include its physical, technological, human, and financial capabilities. There is, of course, additional focus on the technological capabilities, otherwise called tools. These tools can be understood as encompassing both hardware and software tools.

Additionally, Infrastructure as a core category and core capability must take into account the concepts that were grouped into key categories, encompassing process, finance, scope and functionality, specialized tools, and potential issues of new technologies such as cloud computing.

6.3.3 Policies

The core category of “Policies” is perhaps the one that is often forgotten whenever one thinks of the capability. Yet, the data shows that the policy should be treated as a separate core capability with its own set of complex requirements that impact all the other core categories or core capabilities.

This core category must take into account two closely related categories with several sub-categories: organisation development and management standards, and organisational policies. Often, one may be tempted to combine these two distinct categories under the banner of policies and procedures. In fact, some participants discussed policies as being part of the standards they already follow such as ISO.

It is important, however, to distinguish between “organisational development and management standards,” the use and benefit of which cause disagreement among the participants and usually aim at the quality of the DF investigation; and “organisational policies” that govern actions and interactions within the digital forensic organisation. To make it clear, these categories often overlap. But generally, organisational policies deal with what can and cannot be done inside the DFO, while organisational standards deal with setting the standard for quality in either setting up or managing a lab.

6.3.4 People

The core category of “People” is another core capability that is widely recognised by the participants but its importance remains unappreciated, especially at the dimensional level. This includes factors such as the minimal number of staff or investigators that a DFO must have. This also includes taking into account the type and quality of the knowledge and background, education, experience, training, and personal characteristics.

Some participants, further, recognised that the people and the human factors are what make DF work effectively. In other words, it is the people and not the technology that creates successful DF investigations.

6.4 Relationships among the Categories and Core Categories

This section discusses the relationship between the core categories: Investigation, Infrastructure, People and Policy, in order to show the interconnection between the four capabilities. Aside from the richness of the data as discussed previously in this chapter, it is these strong connections among the core categories, especially as they connect down the path at the dimensional level that make them stronger and give them theoretical relevance.

To make the analysis of the relationships deeper, this section discusses each core category pair relationship separately by addressing (1) investigation and infrastructure, (2) investigation and policies, (3) investigation and people, (4) infrastructure and policies, (5) infrastructure and people, and (6) policies and people.

6.4.1 Investigation and Infrastructure

There are many links between the core categories of investigation and infrastructure, such as the investigation process relies on the tools used and relying of most DF investigators technology to conduct the investigation. The shown above about the forensics analysis software, for example, that most DF investigators rely on FTK, Encase, and Xways to conduct forensic analysis. Validation and verification as part of the investigation procedure also rely on the tools for verification of the results by cross checking the results using different tools.

Obvious relationships are the phases of the investigation process (preservation, identification, analysis, and reporting) that are very much dependent on the tools. Specific tools and equipment are needed, for example, to conduct imaging and to protect data from alteration with write blockers. Procedures, therefore, in the investigation process must take into account the available technological infrastructure. Concerns with infrastructure cost and budget may, therefore, impact the investigation process quality and efficiency.

An obvious relationship between, of course, is that the physical infrastructure of a DFO has to take into account the investigation process and procedures, especially the scope of the investigation services, when designing and managing a DFO. The design of the physical

infrastructure together with technical infrastructure must take into account how security breaches might affect the integrity of the investigation process.

6.4.2 Policies and Investigation

The core categories of investigation and organisational policies have a strong link mainly because the core category of investigation is process driven. This means that certain standard procedures or polices must be followed. An example is the statements in the ACPO Principles, which are, in essence, policies about how an investigation must be handled.

There are, therefore, policies relating to each of the phases of the investigation process. Policies are also in place regarding the documentation of the process to maintain a record of the chain of custodies. This may also include policies related to forms, and an access to the investigation laboratory. Some policies will pertain to the people involved in the DF investigation process, whether an investigator or a lab manager will use such policies as confidentiality and technology.

The investigation process itself could shape and dictate the type of policies that a DFO adopts, all of which are dependent on the size of the DF lab. A smaller sized DFO and lab may require fewer policies, while a bigger one may require of more detailed types of policies to protect the integrity of the investigation process.

6.4.3 Investigation and People

The core category of investigation and people relate to each other because people conduct the investigation (the action and interaction) in a DF laboratory also conducts the activities of running the DFO. The strongest (connection) suggestion or argument is that people must hold certain qualification in order to conduct a DF investigation. Therefore, concepts relating to the background, skill, education, and experience of the DF investigator will impact the performance of the investigation. One concept that emerged from the data is the idea of requiring accreditation of DF investigators.

Another link between these two core categories is the training and development of the people in the DFO. How often should the training be given, and will the training be sufficient qualification to conduct a proper investigation.

The human resource management side of people also relates to the investigation core category as issue such as the number of investigators will affect the investigation process.

6.4.4 Policies and Infrastructure

The core category policies is related to infrastructure because, the need to control the use of technology and the physical structure. Policies, therefore, are needed to regulate access control and accountability for access to the DF lab. Further, policies need to regulate the use of technology in the lab such as an isolated network policy for cell phone use policy, wireless connectivity policy, and those policies related to storage and sharing of data. Overall, policies that consider and relate to the security of the infrastructure are also important.

Also a maintenance policy making sure that the infrastructure remains secured. There are also policies relating to the servicing, use, and training on DF forensics analysis software.

Additionally, there are policies relating to the building and managing of the DFO, including the laboratory. A policy should address the design and implementation phases of the lab development, including decisions that balance the scope and infrastructure capability with budget and costs.

6.4.5 Infrastructure and People

The core categories of infrastructure and people relate mostly in regards to the use of the technology infrastructure and access to the physical infrastructure. With regards to the technology infrastructure, the relationship lies at the matching of the people to the tools. There was ample data showing people’s preferences, for example, as to a forensics analysis tool; some prefer FTK over Encase and vice versa.

After all, it is the people that use the tools and equipment. Therefore, the qualification of people, conducting a DF investigation, must be determined. The number and variety of tools in a DFO will also be decided by the DF investigator.

Still, there exists a view that the DF industry focuses on the people's ability over the tools while the data implies that the DF industry and these are very much driven by the tools vendors like Guidance Software for Encase and Access Data FTK.

6.4.6 Policies and People

The core categories of policies and people are also most important because the governance of people seems to be one of the main purposes of the policy. Policy, processes and procedures, therefore, shapes what people do and how they interact with the DFO, DF facility, and the infrastructures in place. Policy will govern what people can and cannot do in order to create a quality and standardised processes. Policy will dictate how people will conduct the investigation processes, and how they will use the tools at certain stages of the investigation.

Policies also shape the quality of the people themselves by setting out minimum requirements for qualification and training. Policy dictates what kind of background a DF investigator must have, how many years' and types of experience they must have, and the type of experience. Like the ones that encourage self-education and play time could affect the DFO's creativity and results.

Finally, a good policy (over people) affects the security of the DFO and also protects the integrity of the data. Good policies will govern how people use the lab, their personal mobile phones and email, and how people use DFO tools and equipment. To be remembered that it is the policy that will shape the quality of people, and the quality of the service and the results of the DFO.

6.5 Conclusion

The discussion in this chapter is about the findings on the subcategories, categories, and core categories and the relationships among the core categories paving the way for a theoretical discussion in the next chapter. This chapter also explained the meanings of the grouped concepts as they were labelled under subcategories and categories, and the meaning of the grouped categories as they were labelled core categories. An understanding of the categories and core categories as they relate and interconnect are essential in order to have a better understanding of the literature as they are applied in the next chapter to support the researcher's proposed theory on DFC.

Chapter Seven: Theoretical Discussion: Towards a Theory on Digital Forensics Organisation Capability

7.1 Introduction

The aim of using Grounded Theory in a research is to propose a theory (Strauss and Corbin, 1998). But first to be asked "what is a theory?" According to Thornberg and Charmaz (2012, p. 41) "a theory states relationships between abstract concepts and may aim for either explanation or understanding". Following this definition, this chapter offers a theory, including a framework, which expresses the relationships among abstract concepts in DFOs that were derived from categories and grouped as core categories at more abstract levels, for the primary purpose of explaining and understanding the development and management of DFO capabilities.

The journey towards this theory is through the coding processes of GT methodology. After reviewing the data and a discussion of the findings in Chapter 6, four core categories emerged from a number of categories and subcategories from the coding processes of GT. These four categories are (1) Investigation, (2) Infrastructure, (3) Policy, and (4) People. Chapter 6 discusses the relationships among these core categories at the dimensional level giving insight into their interrelationships. Therefore, in this chapter, the aim is to take the findings from and discussion of the data from the previous chapters and relate the findings at a more abstract level of theory formation.

This chapter first discusses the four core capabilities as a set of equations starting from the equation, P2 (P1 + I1 + I2) = C. Where P is the policy and C is the capability, I1 is the infrastructure and I2 is the investigation. This reflects the emphasis on applying a policy for every step in building and manging DFC, represented by multiplying the set of polices (P2) to the sum of people (P1), Infrastructure (I1) and Investigation, (I2) core capabilities of which equals capability (C). The section then explains the features of the four core capabilities as a comprehensive framework for DF capability development and management. The chapter then grounds the theory to the data by discussing DF capability

according to the data, which reveals the four core categories as essential. The chapter then connects the DFO core capabilities to existing literature by discussing primary and emerging research on defining DF capability. The chapter discusses the literature on DF readiness (Mouhtaropoulos et al. 2014; Grobler, 2006; Rowlingson, 2004), best practices in building and managing a DF laboratory (Jones and Valli, 2011), the capability maturity model (Hanaei and Rashid, 2014; Kerrigan, 2013; Krutz, 2004), and the Digital Forensic Management Framework by (Grobler, 2011).

7.2 Digital Forensics Organisations Core Capability Framework

This research is developing and presenting formula, equation and a theory for Digital Forensics Organisations Core Capability (DFOCC), and a DFO tool for the development and management of its capability. It is important to identify at the outset that the DFOCC does not offer all the answers for the development and management of a DFO's capability. This type of assignment is beyond the capability of this research. Instead, the main aim of the DFOCC, as discussed in this research, is to make logic of the patterns discovered from the data findings. In other words, DFOCC is a theory which is grounded in the data. It is a framework stated as a theory regarding the capability of a DFO. The theory is stated in terms of equations that express the relationships and roles of the four core capabilities of policy, people, infrastructure, and investigation.

The section below discusses the significance of having identified these four core categories, mainly which they are suggesting a comprehensive framework for developing and managing a digital forensic organisation's capability. The discussion in this section paves the way for further discussion of how the framework can be grounded for the data, and then compared to the existing literature available on DF capability.

7.2.1 The Framework as a Set of Equations

It may be easier to understand the relationships between the four core categories when expressed in the following mathematical equation. In this equation, P1 means People, I1 means Infrastructure, I2 means Investigation, P2 means Policy and C means Capability:

$$\boldsymbol{P2\ (P1 + I1 + I2) = C}$$

The specific meaning of each of the four core categories can best be understood by looking at the categories, subcategories, and phenomena under each core category. (cf. Chapter 6). Capability (C) here is intended to mean a DFO's capability.

Under this equation, the DF capability of an organisation is achieved by multiplying the Policy (P2) to the sum of People (P1), Infrastructure (I1) and Investigation (I2). Capability, therefore, can be achieved only with policy. Policy becomes a primary multiplier because each of the other three categories should not be present without policies in place. Furthermore, having policy as a multiplier means that there is another representation for partial relationship as follows:

$$\boldsymbol{P2P1 + P2I1 + P2I2 = C}$$

In other words the core capabilities: People (P1), Infrastructure (I1) and Investigation (I2) can be regarded distinctly; nevertheless each must also be with the policy multiplier. For instance, one cannot have an infrastructure capability without policy in place to govern the use of facility, maintenance, access control, and any item that belongs to the organisation.

Additionally, a sub-equation emerged concerning the comparative weight of the capabilities. The equation is as follows:

$$\boldsymbol{P2P1 + P2I1 = P2I2}$$

This equation means that the capability of People and the capability of Infrastructure, when added, equal the capability Investigation. DF investigators and managers who use the hardware, software and physical lab etc. (Infrastructure) aim to achieve a successful Investigation. Policy always remains a key multiplier for people, infrastructure, and investigation.

7.2.1.1 Organisational Capability Definition

The above DFOCC equations can lead to many observations and statements about DF and DF capability development and management. One key observation and statement leads to a proposed definition of a DFO's capability:

> **"A digital forensics organisation's capability is the sum of a digital forensics organisation's core capabilities of people, infrastructure, and investigative capability governed by a comprehensive set of policies leading to a unique capability"** (Almarzooqi and Jones, 2016)

The above definition is an expression of the equation taken from the theoretical statement regarding a DFO's capability.

It must be said, however, that the above proposed definition does not aim to fix a complete standard for all DFOs; but it can be an initiative for a new standard in the field of DF specifically defanging DFOs. As stated by Jones and Valli (2011), the minimum requirements of a DFO will depend on factors like budget and scope of the organisation's service. What the above definition requires is that all DFOs should consider the four core capabilities as presented above. An organisation, which does not have any policy for governing personnel, could not be considered capable regardless of the quality of people and technology in the DFO.

The basic or A-Z requirements for each of the four core capabilities are beyond the scope of this thesis. However, some preliminary observations did emerge in the data, and is discussed in more detail below, and which aims to ground this framework to the data.

7.2.1.2 The Role of Policy in Organisation

The framework also suggests that policy must be present in all aspects of capability within a DFO:

> **"A digital forensics organisation must have a set of policies in place governing people, infrastructure, and the investigation to be considered digitally forensic capable"** (Almarzooqi and Jones, 2016)

Policy is involved at the organisational level and has been recognized by scholars in the field of DF. "Organisational policy, such as an overall forensics policy, should form the basis for DFR" (Taylor et al., 2007a; Rowlingson, 2005; Yasinsac and Manzano, 2001)". Organisational policy plays an important role in the DF readiness. All the above clearly identifies the necessity of policy in all the core capabilities, it is therefore clear that organisational capability is not achievable without policies. This is not to say that an organisation does not need to meet all the accreditation standards (Watson and Jones, 2013), rather, this statement says that there must be a set of policies for people, infrastructure, and investigation, regardless of how extensive that policy would be.

DFO's should consider adopting policies at the minimum, across the core capabilities that enhance the quality of evidence. An example of such policy is access control, which supports the credibility and reliability of the entire organisation and the resulting data evidence. ASCLD's essential requirements could be good starting point for any DFO (ASCLD, 2016). These crucial requirements are "the standards which directly affect and have fundamental impact on the work products of the laboratory or the integrity of the evidence" (FBI, 2015).

7.2.2 Application of the Framework

An important question which cannot be ignored is why the DFOCC is important and how will it be valuable in the DF field?

The DFOCC equations mentioned in the above sections can be used to develop and manage a DFO; first as a tool for establishing its capability, then the DFOCC software which was developed during this research to apply the framework in real life. The aim of developing this software was to apply DFOCC in real life by creating a guideline for those wishing to establish DFC. DFOCC software was developed using simple interactive method using C

sharp (C#) programming language. This allows the user to build his capability by answering a series of questions related to the core capabilities he wishes to develop and after that the software produces a report which will include the client requirements for each capability. DFOCC could improve evidence admissibility and also improves the organisation's management operation by increasing the efficiency and effectiveness of its processing. Finally, the DFOCC can set a universal benchmark for the capability of the DFOs taking into account different sizes of organisations.

7.2.2.1 Digital Forensics Organisation Core Capability (DFOCC) Software

Introduction:

This section provides the DFOCC software. It explains how the software was developed, why it was developed and how it works. The software was developed in accordance with development of the DFOCC framework presented in this thesis. This software helps the application of the DFOCC framework in the practical life.

One of the problems discussed here is the absence of a unified standard for the purpose of building and manging DFC, therefore this research was conducted and a framework and software was developed in order to find a solution for building a DFC. Although this software does not provide a standard for building and managing DFC, it provides users with the facts/questions needed to be taken into account when building and managing DFC. The software was designed and built according to the facts/questions derived from data collected in this research involved 19 interviews and visiting over a dozen of organisations.

This software is designed similarly to the survey and questioners applications; it takes the users through a journey consists of four stages. Each stage consists of a number of questions and with each the user is given number of answers. The user is not only guided with suggested answers for each question but also allowed to add his answer according to his need. All four sections of this software are discussed in details in the next sections.

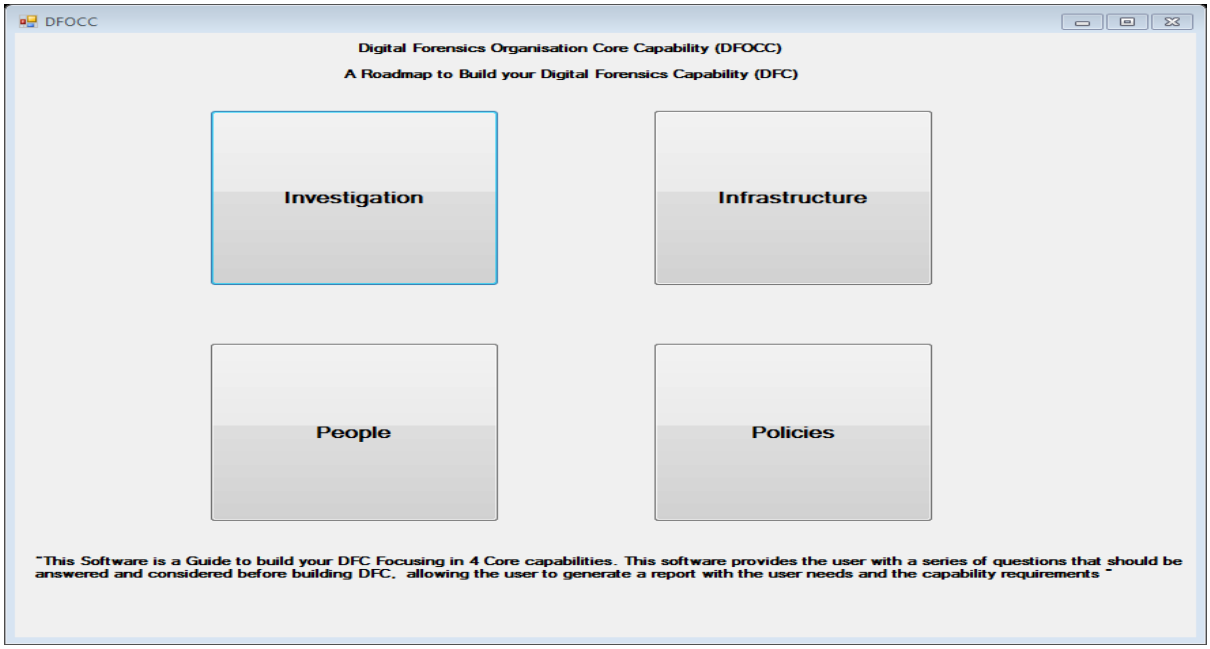


Figure 4 DFOCC Software Main Page

Investigation:

This section includes 16 question/issues divided in three categories: Investigation Process, Investigation Procedure and Evidence Admissibility; the user should answer or consider answering all of them. Below is a screen shot of the investigation section in the DFOCC software?

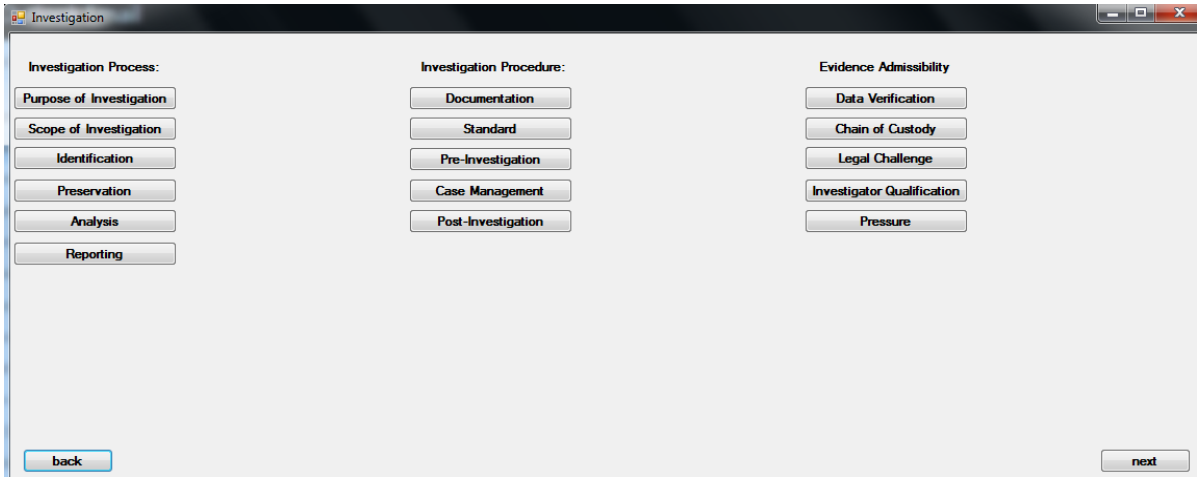


Figure 5 Investigation Page in DFOCC

Attached to each button is either a question or concern where the user is given a drop down list of answers which might suit his need or can add accordingly. User selections are saved in a table in the database as he moves along.

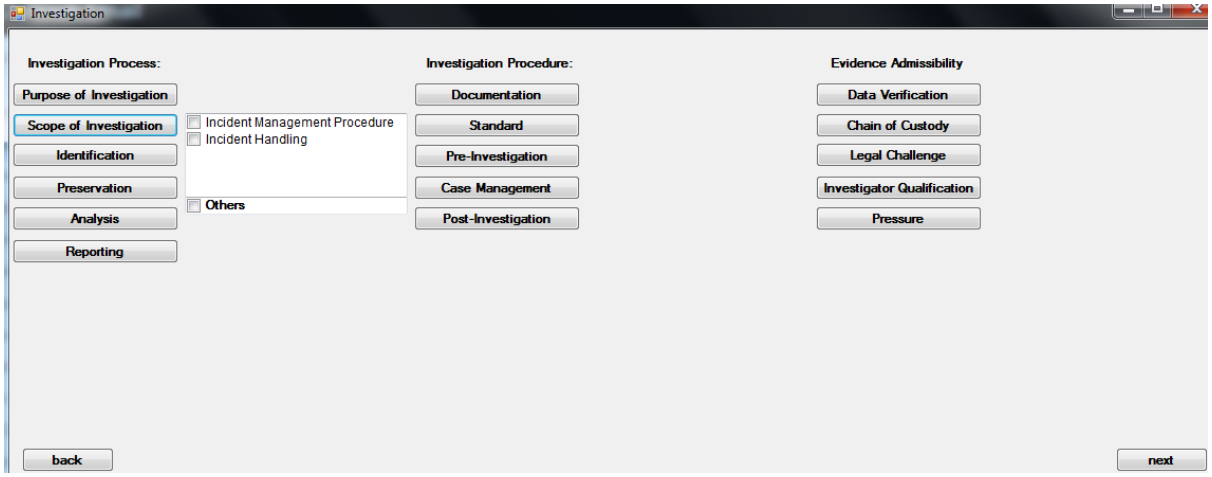


Figure 6 Screenshot of Drop down list for the questions

Infrastructure:

This section is where the user has to consider issues related to the physical and logical infrastructure of the organisation:

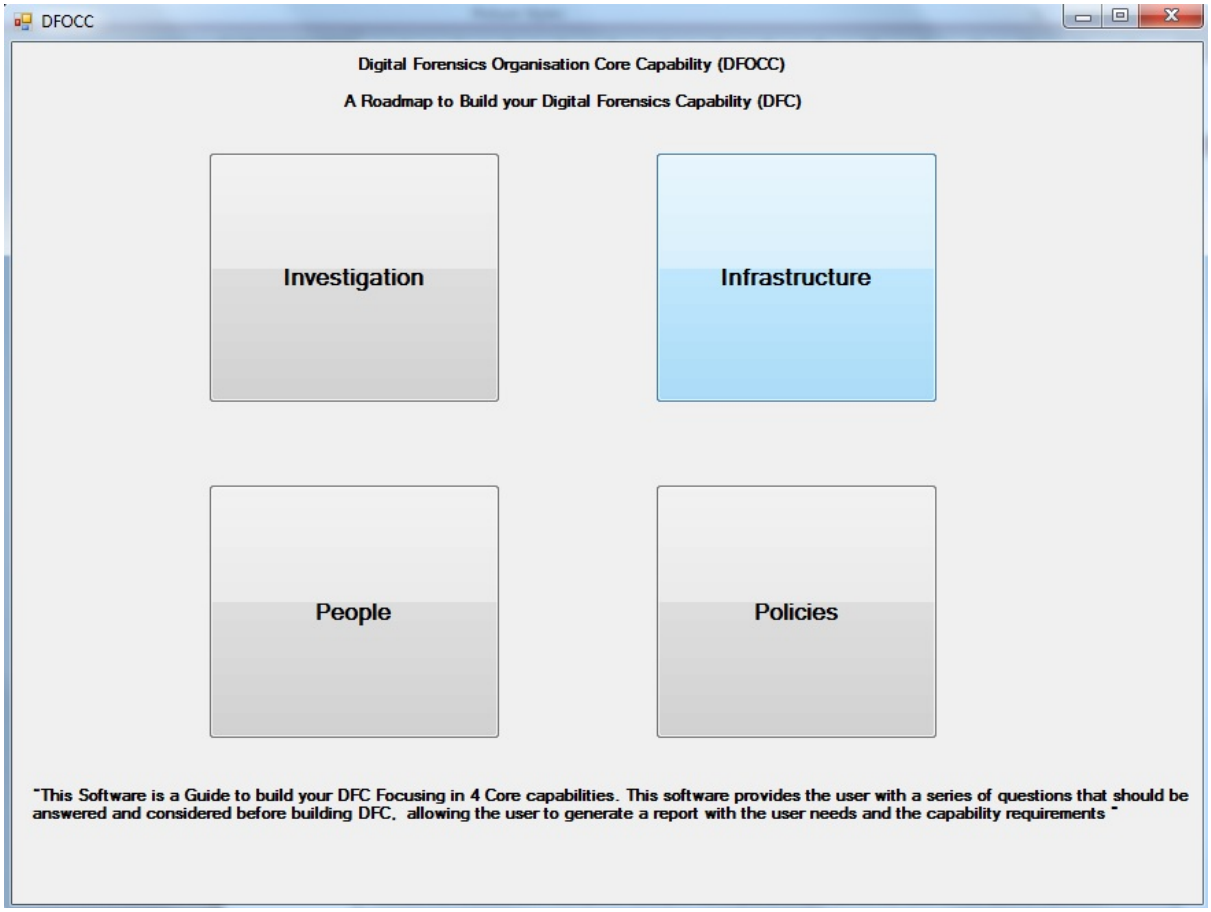


Figure 7 Infrastructure

Infrastructure includes eight questions in three categories as shown in the figure below (Tools, Building a Facility and Cloud Environment):

Figure 8 Infrastructure Categories

People:

This section provides 19 questions divided into six categories: Knowledge, Education, Experience, Training & Development, Organisational Hierarchy and Investigator's trait. DFOCC presents a number of questions related to the personnel in DFC. For example in searching for person to hire, do one requires to know their background knowledge, knowledge on information technology and if one requires such person what qualification one should be looking in him such as university degree that a short course(s) is enough ?

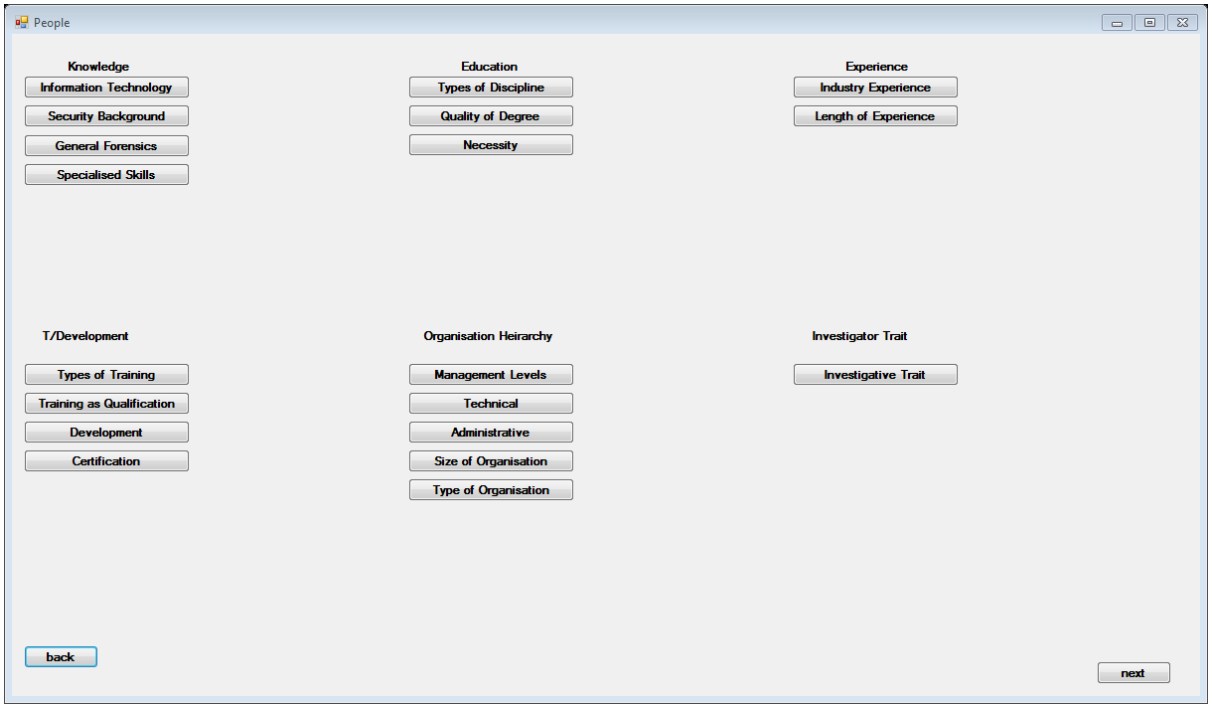


Figure 9 People Categories

Policy:

This is the final section of the software where the user is asked to choose appropriate policy for his organisation. This section has seven questions divided into two categories. This section of the framework is created in order to ensure the existence of a policy that governs the process within the organisation.

Figure 10 Policy Category

Result and Conclusion:

The software saves the user's selections and records answers into a database built in the software from where he can retrieve at the end by asking the software to generate a PDF report. This report is designed and produced to help the user build his own DFC using his answers.

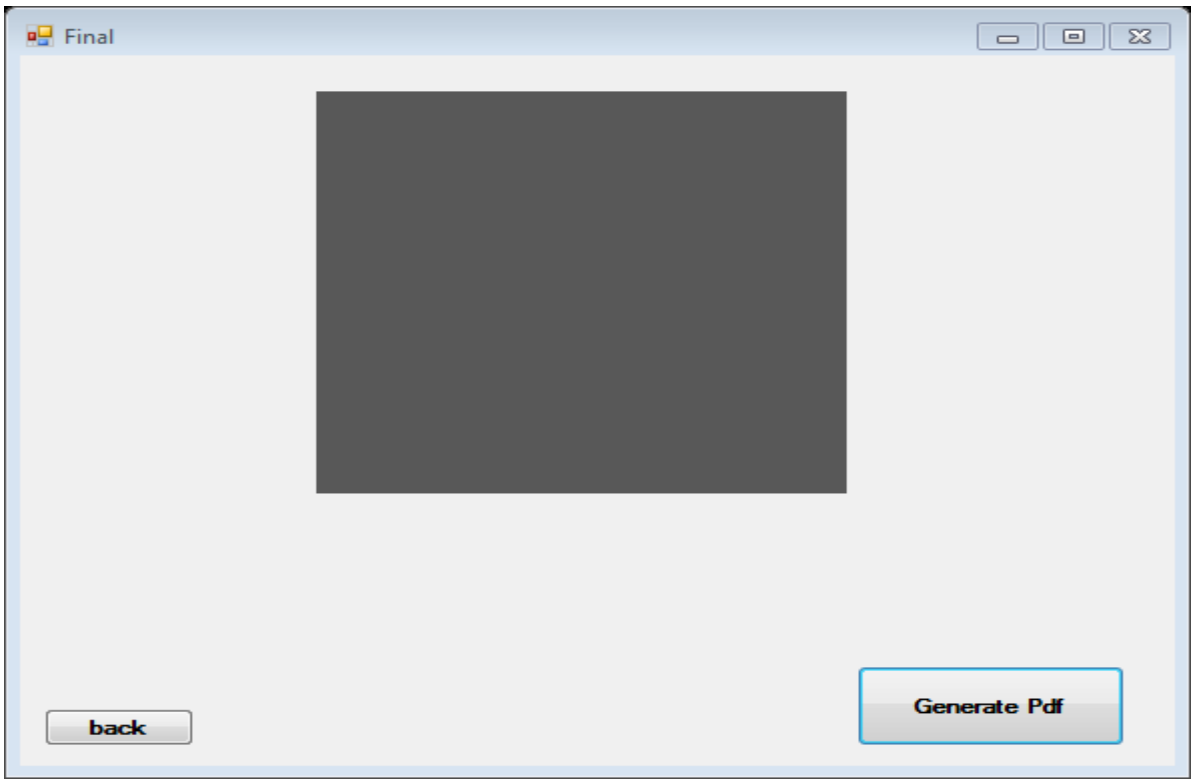


Figure 11 Report Generating Page

Investigation	Infrastructure
--->Incident Handling Pre-Investigation --->Evidence Status	Forensic Analysis Software --->Open Source Process --->Requirement Analysis
People	**Policies**
Specialised Skills --->Task based jobs ----------	Lab Accrediation --->-Reason for accreditation Technology Use --->-Use of Mobile Phones

Figure 12 Final Report Generated from the Software

7.2.2.2 Creates a Roadmap for DFO Development

Currently, there is no standard framework available for those wishing to build a DFO. This observation is validated in the data when the participants were asked the following question: *"Do you know any guideline for developing a digital forensic* [capability]*, a standard guideline?"* (05BJINTUK14p1). Majority of participants indicated that there is no standard in the industry for developing or managing DF capability. (cf. Chapter 6, 6.2.1.7.1). However, Some participants did mention the ACPO Managers Guide and best practices stemming from the ISO and ASCLD, but most recognized them as unrelated directly to the building and managing DF capability especially that there is no one way of establishing and managing DFC (cf. Chapter 6, 6.2.1.7.1.).

Literature presents best practices in building a DF laboratory including some guidelines. Jones and Valli (2011) wrote one of the best books: "Building a Digital Forensics Laboratory: Establishing and Managing a Successful Facility" other book entitled "Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practices Requirements" by Watson and Jones (2013). Both serve as a complete guide for what are needed to build a DF laboratory or facility. Furthermore, the book addresses the organisational needs of DF, including policies and procedures, while distilling the best practices and accreditation standards in the industry (Watson and Jones, 2013). In essence, these books serve as an invaluable one-stop-shop for all the needs of a DFO.

What the DFOCC framework contributes in addition to the work by Jones and Valli is to provide a framework for sorting through a complete list of what one may need when developing a DFO. Jones and Valli do not suggest, neither do Watson and Jones, that a DFO must adopt all the proposed capabilities presented in the books. Instead, they identify the financial limitations and scope of the DFO and show how a DFO will adopt the set of capabilities mentioned in the books. According to the FBI, "The fact that a laboratory chooses not to apply for [ASCLD] accreditation, does not imply that a laboratory is inadequate or that its results cannot be trusted" (FBI, 2015). What the books by Jones and

Valli and Watson and Jones provide is an “inventory”, so to say, of what a DFO may or may not need according to their requirements (Almarzooqi and Jones, 2016).

Regardless the above, literature lacks a guide on how to select the suitable capabilities for a DFO in order to achieve the least requirement. Furthermore the challenge is that defining the minimum requirement is according to the needs of the stakeholders (Jones and Valli, 2011).

The DFOCC provides a roadmap which can be a guide for taking decision in different process of DFO. The DFOCC framework, for example, states that DF investigation requires people, infrastructure, and a policy for the investigation. The DFOCC does not enforce a specific policy because that would be determined by organisation.

7.2.2.3 Identifies Areas for Success Factors

DFOCC framework can help recognize areas of success in DFO. Applying the framework, could examine key factors of success and match the organisation’s DF capability. This can be done by first asking a DFO what they deem are the keys for success. Then, the DFO can be asked to list all their DFO capabilities according to the equation, and compare whether their capabilities match their key success factors. An example of how this works is as follows:

Question: What do you think is your key success factor?

Answer: Quality of our people.

If the success factor was identified as the quality of people, then People Capabilities and People Policies should be absolutely more comprehensive than the Infrastructure Capabilities and Policies and the Investigation Capabilities and Policies.

The DFOCC framework theoretically gives DFO a methodical way of analysing their capabilities and policies relating to each other. Furthermore, DFO’s could compare between policies and may create higher level of policies that overlooks the organisation, by generating cohesiveness in the process.

7.2.2.4 Creates an Attainable Universal Benchmark

DFOCC framework can be applied in small organisations even though the organisation is run by one person. Because DFOCC framework provides small organisations with organisational standards without any need to register for international accreditation. As one participant puts it:

> "*don't believe you need to be accredited to 27001 or 17025. I think those are good but they're optional. They're a big burden. They are both of them are big financial burdens*" (14ETINTUK14p19)

Additional study is required on this capability to identify public standards in DFOs that can be implemented without the burden of accreditation and this is beyond the scope of this research. For example, FTK and EnCase is used by the majority of this research participants and in fact one participant stated:

> *"They are the industry standards. Everyone uses them, so we have to be able to read and write in their formats."* (14ETINTUK14p15-16)

Such data can establish a solid ground for a quantitative type of research into DF capability while using the DFOCC framework.

7.2.3 Advantages of the Framework

The DFOCC offers number of advantages in comparison to the existing literature. First DFOCC is simple and comprehensive. The framework is narrowed down to four variables: Policy, People, Infrastructure, and Investigation and that's why it is simple. Furthermore, it can be expressed in equation form:

- P2 (P1 + I1 + I2) = C;
- P2P1 + P2I1 =P2I2.

The equation shows the relationships of the core capabilities clearly.

As the framework includes all the capabilities essential for a DFO, therefore it is comprehensive. Both, the data (cf. Chapter 6), and the literature (Kerrigan, 2013; Grobler, 2011) support, that the framework capability must include People, Infrastructure (Technology), and Investigation (Process). The framework considers these three, and adds Policy as a core capability that encompasses all three.

DFOCC framework is interconnected which is considered additional advantage. The framework is interconnected because the capability overlooks all other capabilities. The data in chapter 6 shows that the interconnectedness also occurs at the category, subcategory and phenomena levels. For example number of investigators (a dimension) needed in a lab that affects the People core category, by playing an important role in defining the type and size of the organisation. “Number of investigator” also appears in the “investigation process” to determine number of investigators in system in the DF investigation for the peer review purpose. “Number of investigators” also affects “infrastructure” because according to the number of people the budgeting, building software, hardware, and facility requirements will be determined. Finally “number of investigators” affects also the “policy” because (1) hiring and retaining people, (2) validation and verification, and (3) infrastructure efficiency all need to be governed.

Additionally, DFOCC framework acts in a multi-layer style as it considers different, sizes, types, and scopes of a DFO. It can be applied to an individual type organisation as long as it can recognize the minimum requirements for each core category in DFOCC.

Finally, the DFOCC framework is grounded in data because it was formulated using GT, which allows for the data to lead the research. The core categories or core capabilities that emerged were grounded in the data that created the categories and subcategories. To further demonstrate how the DFOCC is grounded to the data, the next section discusses the data relating to a DFO’s capability according to the data and connecting that data to the DFOCC framework.

7.3 Grounding the Theory: Digital Forensics Organisation Core Capabilities According to the Data

Following the GT coding processes, the data were coded for concepts, which were conceptually put into categories and subcategories. These were all falling into four core categories, from which the researcher came out a story line that integrated the data into a theory. The result of such integration is the DFOCC framework and equations presented above. Therefore, the DFOCC framework, through the GT methodology, emerged from the data. Though the theory is "automatically" grounded under GT methodology (Charmaz, 2015), the researcher finds it valuable to show examples where the theory connects to the concepts and phenomena in the data. This means that the DFOCC framework should be identifiable in the complexity of the data. The purpose of this section, therefore, is to explain how the DFOCC framework can be found in the data.

The concept of capability in the context of a DFO and a DF facility is the heart of the research and the DFOCC framework. The phenomenon of creating capability and the concept of capability is grounded in the data because participants gave responses in the interviews which generated phenomena and concepts related to DF capability, which sufficiently achieved theoretical saturation. In fact, capability became a separate category that emerged from multiple concepts and subcategories. What emerged from the category of capability, however, is the same as the emergence of core categories or core capabilities. In other words, whenever the participants talked about what it means to have capability, the concepts they described, that achieving capability can be categorised into four types: Policy, People, Infrastructure, and Investigation.

7.3.1 Policy as Capability

The data showed that policy was essential to a DFO's capability. Not only did participants talk about the need to have policies and procedures, but also how policy contributes to the capability of a DFO. As to the necessity of policy, participants stated the following:

> *"They must have <u>policies</u> and procedures implemented"* (07COINTUAE14p6)

"Our own internal policies, define the way we handle the data" (09MDINTUAE14p2)

Participants also viewed policy as contributing factor to the DFO's capability, and how it affects the DF investigation process and the DF environment. One participant stated, for example, that:

"They're important not only to capability but also to control what's going on in your organisation. And if you don't have policies in place, then potentially people will…they don't know where their boundaries lies so they can steal data and they're not to be held accountable, for example, so you need policies in place to control your environment and control what people can and can't do" (13NXINTUK14p7)

When participants were asked the following question:

"Do you think these policies help or contribute to your capability?"

The response was an astounding

"They definitely do." (14ETINTUK14p20)

Or

"Oh yes. Yeah. You have to." (15RMINTUK14p33).

This is true, despite the fact that participants gave different reasons as to how policy contributes to capability. Overall a policy capability establishes boundaries.

"Yeah, yeah absolutely. I mean, having the NDAs, confidentiality agreements basically establish, you know, a cross point for you." (08SLINTUAE14p12)

It is also a starting point with regards to how the DFO views itself and its functions. In other words, policy creates awareness about other capabilities of the organisation. As one participant stated:

"It helps staff realize the importance and the sensitivity of the…of the work they're doing and…especially the cases that we're handling…So, it is very necessary to

have these policies in place and enforced on all the employees, reviewed and revised as well on a periodic basis." (11CTINTUAE14p8)

Additionally, one participant stated about the ability to find and secure sensitive or confidential information. As on participant stated,

"*Yes they do because they help us…to preserve our information, our intellectual property and of course client information"* (10KSINTUAE14p8)

As about the roles of policy with regards to the rest of the DFO and other capabilities, the data shows that policy affects the capabilities of people and investigation, as stated by the following participant:

"but as far as procedures that is an essential must cause you have to have documented procedures, you will need to know what you are looking for, training of the people, maintain that level of knowledge is essential and of course and everything from policy." (09MDINTUAE14p5)

The investigation process and the results of that process are impacted by policy because of the way in which the policy can control information leakage through standards and procedures in place:

"It would contribute to our name, as a professional…and it will also contribute to the, the results because if there was no following for standard, we could have information leakage which is not good for any security organisation." (12CTINTUAE14p7)

Policies, therefore, relate to the relationships among the DF employee, DF client, and DFO and impact the ability of the organisation to control information, thereby affecting the people capability.

"…we have nondisclosure agreement and confidentiality agreement for employees and our client to maintain you know the information" (14ETINTUK14p21)

"They're important not only to capability but also to control what's going on in your organisation. And if you don't have policies in place, then potentially people will…they don't know where their boundaries lies so they can steal data and they're not to be held accountable, for example, so you need policies in place to control your environment and control what people can and can't do"(13NXINTUK14p7)

If at all, the existence of policies improves the DFO's relationships with clients and third parties by enhancing trust. One participant explained this phenomenon as follows:

*"So if that's not in place, there's a lack of trust here, you know, usually from the customers. There must be an agreement in place, so they can feel good about it" (*08SLINTUAE14*p13)*

Policy can also be used to improve the infrastructure capability and how a DFO manages the action and interaction between people and technology. One participant stated the necessity of policy on DF technology as follows:

*"With due diligence, there are several policies which go from…not having the mobile to how to control the taking of picture, how to control large storing evidence. I mean, how many law enforcement agencies are applying a policy where they're restricting a screen copy, paste policy" (*03ALINTUAE14*p20)*

Finally, policy enhances the admissibility of evidence as it shows that the DFO has made certain procedures as a part of their business process. One participant explained this added benefit as follows:

"I'm not sure that that contributes to the capability…but I would definitely say that at least is something which is definitely beneficial from <u>a legal standpoint</u> when it comes to dealing with third parties because all of a sudden somebody questions whatever you are doing or raises an issue with confidentiality policies. You can always refer to the policy and say this is what we follow, this is what we do and take the responsibility in a way that is useful for an organisation." (09MDINTUAE14p9)

The data, therefore, shows that policy has an overarching effect on the DFO. The data shows that policy is a separate capability, and that policy affects the capabilities relating to people, infrastructure, and investigation. The data hence justifies the following equation:

P2 P1 + P2I1 + P2I2 = C

This equation means that policy impacts people (P2P1), infrastructure (P2I1) and investigation (P2I2). Policy can also be viewed as a separate capability in the following equation:

P2 (P1 + I1 + I2) = C

The equation allows for policy to be looked as a separate capability that contributes to the entirety of a DFO's capability. Policy as capability, therefore, is grounded in the data.

7.3.2 People as Capability

The data also showed that people was essential to a DFO's capability. Participants talked about the need to have capable people.

"*People, absolutely essential" (*09MDINTUAE14p4)

But the need to have people as capability also requires looking into the quality of the people, the type of background, training, and experience, and the various specialized skills that a DFO may need to created capability.

"*You need capable people"* **(**13NXINTUK14p3**)**

"*Choosing the right people, of course"* (10KSINTUAE14p2, 3)

Participants talked about the need to train people in DFOs:

"*T*raining *of the people"* (09MDINTUAE14p5)

Or

> *"I should be competent to do that and my staff should be competent to do that. And if we don't give them the training they require to do that, then we are morally in big trouble. And legally I don't think we have a leg to stand on either"* (16WPINTUK14p6)

Other participants talked about people as having background knowledge in security:

> *"No, he must have a security background."*(08SLINTUAE14p16)

Or

> *"The information, or at least the knowledge on all basic, all the fundamentals of forensic security" (*11CTINTUAE14p9)

Still, others required specialization in forensics as a team or specialized in various areas that:

> *"You must have a team specialized in forensics"* (08SLINTUAE14p5)

> *"You'd have to have somebody who's specialized in, in various areas. You cannot expect one person to do everything that is required of digital forensics today"* (09MDINTUAE14p3)

Additionally, participants talked about how people contribute to the capability of a DFO. Some participants view people as the primary capability in an organisation. One participant, for example, stated as follows:

> *"The main thing is the people. That is the main thing. And the quality of the people and their education and training"* (05BJINTUK14p4)

> *" which is the most important thing …you must have the person itself" (*08SLINTUAE14*p1)*

Some participants described the capability of people as among the capabilities in addition to or alongside other capabilities.

"Is it, is it the people, technology, facility" (15RMINTUK14p11)

The capability of people was, therefore, related to "policy and procedures" like "chain of custody", the investigation and the investigation process, and technology. One participant explained the interrelatedness of the capabilities as follows:

> *"… They must have policies and procedures implemented, people must know how to handle cases and there must be a chain of custody kept, so they must be prepared for that. They must know exactly what digital evidence received, how they handle this and must be a process already in place. So chain of custody, people who are aware of the technology, and how to use it. And then maybe HR rules and legal rules of how they will handle these investigation"* (07COINTUAE14p6)

Some participants expressed the interrelatedness of the capability of people with the other types of capabilities:

> *"Okay, for a provider digital forensics company they should have enough capabilities in term of human resources, people that have enough experience, working in the field. It's a very good to have also legal side and people who know or aware about what are the rules and regulations in the place that they are working in and a technology awareness, what are the technologies that are available and what are the solutions available."* (07COINTUAE14p4)

> "*Once we had technical capabilities there and also the employees were unable to …the procedures…doing forensic investigation."* (08SLINTUAE14p3)

> "*First, have to follow standard. And it must have tools and equipment and definitely the knowledge. Those three things are…we make a good digital forensics lab and team.*"(12CTINTUAE14p2)

As such, people as capability relates to technology:

> *"you have to have somebody who knows enough of each of the operating systems that are out there and major operating systems that I've used to be able to analyse"* (09MDINTUAE14p2)

> *"You need people and, and then on top of that you…hardware and software…" (*13NXINTUK14*p4)*

> *"Obviously you need the physical equipment to make technical capabilities, but you also need to have the human resources able to do it. So, it's about qualifications and training and appropriate peer review within that laboratory."(*14ETINTUK14p4*)*

One participant stated that the capability of infrastructure, specifically tools, was reliant on the people using the tools.

> *"You need capable people, and I think people are the most important part. You can buy lots of software, you can buy lots of tools, and you can buy lots of training but you need to have an individual and a team of individuals with the right aptitude to do an investigation. And then once you've got those people in place you can give them the software, give them the hardware, give them the training and then build your digital forensic lab" (*13NXINTUK14*p3)*

It also relates specifically to the investigation:

> *"The key success factors, first of all, are to have proficient analysis, investigation analyst…" (*11CTINTUAE14p3*)*

Then, the people capability must also relate to the policies and procedures of the DFO:

> *"Okay, so they must have …policies and procedures implemented. People must know how to handle cases and there must be a chain of custody kept…so they must be prepared for that. They must know exactly what digital evidence received, how they handle this and must be a process*

> *already in place. So chain of custody, people who are aware of the technology and how to use it. And then maybe HR rules and legal rules of how they will handle these investigations" (*07COINTUAE14*p6)*

The data, therefore, show that the DFO capability of people is interrelated to the other capabilities specifically policy, infrastructure, and investigation. The interrelatedness goes to the dimensional level in terms of the number of investigators, and types of policies that are needed. The data also show that the core capability **P1** is separate type of capability and is viewed as such by the participants. The data justifies the following equation, where P1 means people capability, with regards to people as a core capability:

P2 P1 + P2I1 + P2I2 = C and P2 **(P1 + I1 + I2) = C**

According to the DFOCC and as grounded in the data, people (P1) is a separate core capability that combines and interrelates with the other core capabilities (P1, I1, I2) to create the capability (C) of a DFO. People as capability, therefore, are grounded in the data.

7.3.3 Infrastructure as Capability

The data showed that infrastructure was essential to the DFO's capability. Not only did participants talk about the need to have infrastructures, but also the type of infrastructure, and how infrastructure contributes to the capability of a DFO by its interrelationship with other types of capabilities.

Participants understood the distinction between the types of infrastructure capabilities, specifically the distinction between physical infrastructure (facility or lab building) and the technological or technical infrastructure. One participant stated the following distinction:

> *"Obviously you need the physical equipment to make technical capabilities" (*14ETINTUK14p4*)*

Another participant described the infrastructure capability in terms of the facility as a whole:

> *" I guess facilities would be third. The appropriate facilities for the work that you're undertaking. And security"* (14ETINTUK14p10)

> *"If you're designing a lab from scratch or working on one in your country. They want everything. They want the ability to receive evidence, process of evidence both computer and cell phone evidence, fixed physical storage. They also want the ability to disassembly, physical, physical recovery, and training. So all those parts play a part in the design of the physical lab. So, once you've identified what it is you want to do, you then have to identify the physical premises that will allow you to do it. Then you can identify any changes that are required to the physical premises to allow you to obey the standards…so, continuity, security, EXT protection, CCTV, secured storage, fire suppression, all of these things are the first steps in identifying how to build a forensic laboratory."(*14ETINTUK14p5*)*

Other participants emphasized the need for the technology, hardware and software side of infrastructure capability:

> *"Second is the technology, of course" (*10KSINTUAE14*p3)*

> *"You have to the knowledge; you have to have the technology to be able to do some of these things. As far as computer forensics, it's clear enough. You got software that does a lot…" "Then as far as computer hardware goes, specialized forensics workstations." "You have to have the technology to be able to do some of these things" (*09MDINTUAE14p2, 3*)*

> *"And it must have tools and equipment" (*12CTINTUAE14p2*)*

Participants also identified the relationship between people capability and infrastructure capability, especially how people use the technology side of the infrastructure. Participants discussed these phenomena as follows:

> *"…you have to have somebody who knows enough of each of the operating systems that are out there and major operating systems that I've used to be able to analyse…" (*09MDINTUAE14p3*)*

> *"You need capable people, and I think people are the most important part. You can buy lots of software, you can buy lots of tools, and you can buy lots of training but you need to have an individual and a team of individuals with the right aptitude to do an investigation" (*13NXINTUK14p3*)*

One participant expressed that the type of tools, specifically software, does not matter if you have people who understand how the tools:

> *"The software that you're using it doesn't really matter what software you are using if you understand what's going on behind the scenes." (*09MDINTUAE14p4*)*

Another participant explained the need to have other types of capabilities like people and policies with the infrastructure capability:

> *"You need people and, and then on top of that you…hardware and software…and, and then there's lots of peripheries things and…which…it really is a combination of things. So you need hardware, software, training and procedures, standards and guideline" (*13NXINTUK14p4*)*

The participant in the statement above, in essence, relates infrastructure capability with procedures, standards and guidelines under the policy capability.

Another participant associated the infrastructure capability in basic tools to policy and procedures and as part of the investigation process of preservation.

> *"…I think you need some basic tools, so some basic tools to get the data, also to comply with the ACPO principles and the first ACPO principle talks about, you know, not working on the original evidence. So making a copy (*16WPINTUK14p5*)*

*"You need some basic tools to do that, make a copy, and it was not always possible especially with mobile phones…" (*16WPINTUK14p6*)*

*"technical capabilities there and also the employees were enable to know the procedures…doing forensic investigation."(*08SLINTUAE14p3*)*

The data, therefore, shows that the DFO capability of infrastructure is interrelated to the other core capabilities of policy, people, and investigation. The interrelatedness goes to the dimensional level in terms of the quality of the people using the infrastructure and technology; the types of policies, standards or guideline to consider and specific phases in the investigation process like preservation. The data also show that infrastructure is a separate type of capability and is viewed as such by the participants. The data justifies the following equation, where I1 means infrastructure capability, with regards to infrastructure of facility and technology as a core capability:

$$P2\ P1 + P2\mathbf{I1} + P2I2 = C \text{ and } P2\ (P1 + \mathbf{I1} + I2) = C$$

According to the DFOCC and as grounded in the data, people (P1) is a separate core capability that combines and interrelates with the other core capabilities (P2, I1, I2) to create the capability (C) of a DFO. Infrastructure as capability, therefore, is grounded in the data.

7.3.4 Investigation as Capability

The data showed that investigation was essential to a DFO's capability. Investigation, in fact, is the purpose of DF. Not only did participants talk about investigation in terms of the investigation process and investigation procedure, but also how investigation contributes to the capability of a DFO. Participants stated the need for a standard and procedures in the investigation process, which highlights the importance of the phases of the investigation process.

*"First, have to follow standard."(*12CTINTUAE14p2*)*

Participant also stated that the DF investigation related to the other core capabilities of infrastructure technology, people, and policies.

> *"And it must have tools and equipment and definitely the knowledge. Those three things are…we make a good digital forensics lab and team."(12CTINTUAE14p2)*

> *"…it really is a combination of things. So you need hardware, software, training and procedures, standards and guidelines" (*13NXINTUK14p4*)*

One participant highlighted the need for a peer review policy and how policy capability is closely tied to the people capability and the investigation process in the investigation capability.

> *"I think you need to go further than that. For example, we can receive some evidence, store that evidence appropriately and control its access to it appropriately and we can perform forensic analysis to that data and we can produce a report and that report can be accepted by prosecution or defence. That's not necessarily a successful forensic process. What we have to do is have a process of peer review built into it, so even if it looks as though you've found the evidence, the peer, your peer can review the process and assure that the process can't be challenged. So, all the work we do here, although less now because we do less work, but all the work we used to do, whichever analyst did it, including me as the principal analysts. If I produced a report, my senior forensic analyst would then attack that report as if he was the defence."* (14ETINTUK14p5)

Another participant explained how the investigation process related to other core capabilities:

> *"Okay, so they must have policies and procedures implemented, people must know how to handle cases and there must be a chain of custody kept. So they must be prepared for that. They must know exactly what digital evidence*

> *received, how they handle this and must be a process already in place. So chain of custody, people who are aware of the technology and how to use it. And then maybe HR rules and legal rules of how they will handle these investigations"* (07COINTUAE14p6)

Another type of policy that the participants emphasized is the need for a documented procedure. In other words, the investigation capability must also be following the policy capability of documenting the investigation process:

> *"…documented procedures that need to be followed for each, each of them so you can repeat the steps and anybody else can actually verify the report"* (09MDINTUAE14p3)

> *"but as far as procedures that is an essential must because you have to have documented procedures"* (09MDINTUAE14p5)

> *"And you need to have some form of audit trail all within the ACPO Principles and you need to be able to be competent and be able to explain it to an officer, whose job it is that you are working on, what you've done and why you've done it. So, I think that's the basics. Procedures, yeah, absolutely."*(16WPINTUK14p6)

One participant also related the investigation capability to a policy or process for continual assessment:

> *"it needs to be part of the continual assessment process"* (14ETINTUK14p10)

Another participant also related the investigation capability to the people and infrastructure capabilities:

> *"obviously you need the physical equipment to make technical capabilities, but you also need to have the human resources able to do it. So, it's about*

qualifications and training and appropriate peer review within that laboratory." (14ETINTUK14p10)

The data, therefore, show that the DFO capability of investigation is interrelated to the core capabilities of policy, people, and infrastructure. The interrelatedness goes to the dimensional level in terms of the quality of the investigation process using the infrastructure, technology, and policies or standards and procedures. The data also show that investigation is a separate type of capability. The data justify the following equation, where I2 means investigation capability, with regards to investigation as a core capability:

P2 P1 **+** P2I1 + P2**I2** = C and P2 (P1 + I1 + **I2**) = C

According to the DFOCC and as grounded in the data, investigation (I2) is a separate core capability that combines and interrelates with the other core capabilities (P2, P1, I1) to create the capability (C) of a DFO. Investigation as capability, therefore, is grounded in the data.

7.4 Digital Forensics Readiness

DFR has been described in the literature "as the pre-incident plan within the DF Investigation lifecycle that deals with digital evidence identification, preservation, storage, analysis and use whilst minimizing the costs of a forensic investigation. In other words, DFR aims to manage digital evidence in such a way to provide for a timely and cost-effective forensic investigation" (Mouhtaropoulos et al. 2014). Interestingly, they also described the DF investigation process as consisting of the same four phases described in this research: identification, preservation, analysis, and reporting (Mouhtaropoulos et al. 2014).

The key practice of DF preparedness and DF readiness is to ensure that when a DF investigation is carried out, the investigator can find the relevant results in a timely manner (Cruz-Cunha, 2014, p.415; Rowlingson, 2004). According to Rowlingson, DF readiness is "the ability of an organisation to maximize its potential to use digital evidence when required" (Cruz-Cunha, 2014, p.415; Rowlingson, 2004). "In the context of enterprise

security the definition of forensic readiness can be broadened to: the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation" (Rowlingson, 2004).

Nevertheless, DFR remains a main factor of the DF investigation process as the application of DF readiness supports the DF investigator before a crime takes place. DFR is, therefore, proactive rather than reactive. An example of a DF investigation framework that takes into account DF readiness is the DF control framework suggested by Von Solms et al. (2006) as a governance framework for the DF investigation process. Again, like DF readiness, the DF control framework does not report a DFO's capability to establish or run a DFO.

7.5 Capability Maturity Model

The capability maturity model (CMM) has recently seen its application to the field of DF in two ways: at the DF investigation and at the DFC perspective. Before clarifying the limits of the CMM in clarifying DF organisational capability, it is important first illustrate CMM and its roots. Second, this section discusses the application of CMM in DF investigation. Third, this section also explains the recent application of CMM to DF capability. Finally, this section shows how the CMM complements a DFOCC, but does not by itself achieve a comprehensive view of DF capability.

According to Kerrigan (2013), the CMM is used to "describe the degree to which an organisation applies formalised processes to the management of its various business functions. CMMs provide guidance for organisations to define their business processes and improve those processes over time." CMM uses a five level of maturity in defining the capability level of an organisation's processes. The CMM applied first in software engineering as assessment tool to measure the ability of government contractors' in building software's (Kerrigan, 2013). It was later successfully applied to other disciplines or process areas as a framework for process improvement.

Krutz (2004) first applied CMM to computer forensics in a US Patent application, which was published in 2006 and abandoned in 2008. Krutz defined CMM in computer forensics as follows:

> "*A method of defining an architecture for a computer forensics capability and maturity model, whereby said architecture is to be used for assessing capability and maturity of an organisation's computer forensics processes, said model comprising: a. establishing a plurality of process areas relating to the domain of computer forensics; b. establishing a plurality of computer forensics base practices, each corresponding to a fundamental characteristic that is practised in the computer forensics domain; c. correlating the base practices to the process areas, whereby related ones of said best practices are respectively grouped as a subset within each process area according to a common purpose.*"

In Krutz's model, there were 36 identified processes that could be assessed in terms of five levels of maturity: (1) informally performed processes, (2) planned and tracked processes, (3) well-defined processes, (4) quantitatively controlled processes, and (5) continuously improving processes (Krutz, 2004). Krutz's major shortcoming was that his application of CMM was to computer forensics, and therefore did not cover the broader discipline of DF (Kerrigan, 2013).

As a reaction to Krutz's shortcomings, Kerrigan (2013) applied the CMM to DF investigations after reviewing the various DF investigation frameworks and models in the field. Kerrigan's proposal was to create "a tool with which to benchmark the capability of the industry regulators" (Kerrigan, 2013). In doing so, Kerrigan specifically noted that the CMM had to be applied keeping in mind three important and interrelated concepts: People, Process, and Technology (Kerrigan, 2013). Kerrigan, like Krutz, designated five levels of maturity: (1) Ad-hoc, (2) Performed, (3) Defined, (4) Managed, and (5) Optimised (Kerrigan, 2013). The five levels were then applied to the three key factors of organisation capability to conduct DF investigation: Process, People, and Technology. Of the three key factors, only processes were broken down to smaller types of action or interaction.

While Kerrigan extended CMM to DF investigation, Kerrigan did not apply CMM to a DFO's development and management capability. In other words, the focus was on the process of investigation. An advantage to Kerrigan's model, on the other hand, is that it

identifies the role of technology and people in the investigation process. Kerrigan, nevertheless, failed to state specific actions/interactions in the "People" and "Technology" categories that would clarify the relationships among the categories.

Another application of the CMM to a DFO's capability is the model proposed by Hanaei and Rashid (2014). The CMM model gives six levels of maturity: (0) Person Dependent Practices, (1) Documented Processes, (2) Partial Deployment, (3) Full Deployment, (4) Measured and Automated, and (5) Continuously Improving. These levels are largely similar to that proposed by Kerrigan. Additionally, like Kerrigan, Hanaei and Rashid's model takes into account the improvement of the process, tools (technology), and skills (people). Also like Kerrigan, this CMM model does not address a DFO's development and management capability, and did not explain with specificity how the tools and technology are to be enhanced.

One reason for the CMM models' silence on the detailed relationships and requirements of technology and people lies in the inherent limitation of CMM in explaining a DFO's core capability, especially with regards to development and management. Instead, CMM mostly focuses on the procedure because it was created primarily to improve the business process, unlike the DFOCC where it focuses on policy. To conclude, CMM is focuses more in improving processes in the existing organisation, it is does not consider the process of establishing organisation's capability from scratch and in defining a minimum requirement for DFC.

7.6 Digital Forensics Management Framework

Perhaps the most relevant literature on DF organisational capability is the Digital Forensics Management Framework (DFMF) suggested by Grobler (2011) which proposed the DFMF as a comprehensive approach to DF investigation. This section discusses the DFMF as rooted in a multi-dimensional view of DF, and how it is similar to the DFO core capabilities identified in this research. This section then discusses how the DFMF differs from the DFO core capabilities proposed in this research. Finally, this section explains how the DFMF confirms the DFO core capabilities.

7.6.1 DF as Multidimensional Discipline and DFMF

Based on a multi-dimensional approach to DF (Reddy and Venter, 2013; Grobler and Louwrens, 2006), the authors engaged individual actions in a complete DF investigation model to find the scopes of DF:

> *"We will use the dimensions of DF, legal and judicial, management or governance, policy, process, people and technology related activities or deliverables to categorise the individual actions"* (Grobler, C, 2011, p. 8-209)

This researcher then constructed DFMF based on these dimension. The dimensions identified were "legal and judicial dimension", "governance dimension", "policy dimension", "process dimension", "people dimension", and "technology dimension". Interestingly, some of these dimensions match the core categories identified in this research from the data analysis using GT. Table 19 compares DFOCC and the dimensions of DFMF.

DFOCC	**DFMF**
Policy	Policy
Investigation	Process
People	People
Infrastructure	Technology
	Legal and Judicial
	Governance

Table 18 DFOCC and DFMF

Table 19 shows the differences between the DFMF and the DFOCC methods to DFC. The next section discusses in more detail the similarities and differences between the two.

7.6.2 Similarities between DFMF and DFOCC

The DFMF and the DFOCC have a number of key similarities that are worth exploring in detail. A glance at the DFMF and the DFOCC seems to reveal basic similarities on the existence of the four core capabilities for a DFO: Policy, Process, Investigation, and Infrastructure. The DFMF has two additional dimensions: “Legal and Judicial” and “Governance”, on the other hand DFOCC acknowledged those Legal and Judicial” and “Governance” by using the conditional matrix as affecting competence and not core capability. It is clear that the wordings are different; DFMF uses “Process” and “Technology”, while DFOCC uses “Investigation” and “Infrastructure”. Looking at the requirements of the DFMF and deliverables level discloses a number of concerns especially when comparing the categories and subcategories identified in the DFOCC. Table 19 compares DFMF and DFOCC (requirements and deliverables in DFMF Vs Categories and Subcategories in DFOCC):

DFMF Deliverables	DFMF Requirements	**DFMF Dimensions/DFOCC Core Categories**	DFOCC Categories	DFOCC Subcategories
	Evidence Handling and Management Policy	**Policy**	Facility Building and Management Standards	Standards
				Best practices
				Guidelines
				Lab accreditation
				Ad Hoc
				Key Success Factors
	Incident Management Policy		Organizational Policies	Information Security Policy
	Education, training, and awareness policy			Physical Security Policy
	Management Policies			Tech Use Policy
	Infrastructure Policies			Maintenance Policy
				Confidentiality & Non-Disclosure
				Evidence Storage Policy
				Conflict of Interest
				Operational Manual
				Policy as Capability
				No Policy
				Ethics Policy
				Standards/Accredit

				ation
Evidence Management	Evidence Handling Procedure	Investigation / Process	Investigation Process	Purpose of Investigation
Digital Evidence				
Physical Evidence				
Post incident evidence				
Incident Handling	Incident Management Procedure			Scope of investigation
Investigation procedures				Identification
				Preservation
				Analysis
				Reporting
				ACPO Principles
BIA	Risk Management/Contingency Procedures		Evidence Admissibility	Data Verification and Validation
IRP				Chain of custody
DRP				Qualification of Investigator
BCP				Expert Testimony
New Technologies				Vulnerable to Legal Challenge
				Authentication
				Data Verification

				and Validation
General Management	Management Procedures		Investigation Procedure	Documentation
				Standard (ASCLD)
Use of DF for non-DFI purpose				Pre-Investigation
				Case Management
				Post Investigation
Operational infrastructure	Infrastructure Procedure			
DFI Infrastructure				
	Code of Conduct	**People**	Knowledge/Background	IT
				Security
				Law
				General Forensic
				Specialization of DF staff
	Awareness Programmes		Education	Type of Discipline
				Quality of Degree
				Necessity
Technical Education and Training	Education and Training Programmes		Experience	Industry experience
First Responders				Experience Means
General				Length of

User				Experience
Management			Training and Development	Types of Training
Investigator				Training as Qualification
Expert Witness				Development
				Certification
				Self-Education
				Necessity
			Organizational hierarchy	Management
				Technical
				Administrative
				Size of Organization
				Type of Organization
			Investigator Trait	Investigative
				Communicative
				Technical
				Analytical
				Motivated
				Creative
				Aptitude
				Security Clearance
				Quality of people
IDS	Operational	**Infrastructure**	Tools	Tool selection

Systematic Gathering	Infrastructure	**/ Technology**		Forensic Analysis Software
Monitoring				Standard tool
Networks				Hardware
Time synchronization				Software/Hardware
				Peripherals or Accessories
				Small Scale Devices
Hardware	DFI Infrastructure		Building a DF Facility	Process
Software				Facility Requirements
Miscellaneous				Financial
				Functionality and Purpose
			Virtual Environment	Cloud

Table 19 Similarities between DFMF and DFOCC

Table 20 show the data which emerged after applying GT which shows consistency with previous scholarly work in the field of DF, for example the multi-dimension approach which was used to develop DFMF by Grobler. This approach originated from literature, which Van Solms has recognised as a multi-dimensional discipline. “Von Solms identified various dimensions for Information Security: People, Policy, Risk Management, Legal, Ethical, Insurance, Technology, Strategic Governance and Operational Governance etc.” (Grobler, 2006; Von Solms, 2001). For example “Corporate Governance, People, Policy, Legal, Compliance and Technology Dimensions of Information Security” were used to establish an assessment model for Information Security as dimensions (Grobler, 2006;

Grobler and Louwrens, 2006). These dimensions are the common factors between the DFOCC and the DFMF.

There are, however, significant differences between DFMF and DFOCC. One key source of the differences between DFMF and DFOCC is the aim and purpose. The DFMF aims at showing the multi-dimensional aspect of a comprehensive DF management framework, whereas the DFOCC aims to identify a pattern of core capabilities in developing and managing a DFO. In this regard, the DFOCC focuses on building and developing a DFO with a DF lab within the organisation. Additionally, the DFMF and the DFOCC have different applications. The DFMF aims mainly at a management framework, whereas the DFOCC aims at developing a standard for developing and managing a DFO.

Most significantly, DFMF and DFOCC used different methodologies. DFOCC core categories were identified in this research, therefore, came directly from the data and relates to the data and other categories at the properties and dimensional level. On the other hand, the development of DFMF was not systematic and did not involve methodological scientific research and directly came from the existing literature. In such case, according to Ellis and Levy (2009), GT "can furnish additional value when literature fails to support the theoretical evolution of phenomena." (Jones and Alony 2011), making the use of GT in the research even more appropriate.

7.6.3 How DFMF corroborates the DFO Core Capabilities

Despite the differences between DFMF's and DFOCC, DFMF supports DFOCC. The reason behind is because DFMF and DFOCC focus on the four capacities: People, Policy, Infrastructure (Technology), and Investigation (Process). This robust association shows that the DFOCC leads to the same situation as DFMF despite using their own methodology to achieve the objective. Both DFMF and DFOCC stand that any DFO must consider the four core capabilities when making decisions about DF, whether from a management, development, or investigation perspective.

Chapter Eight: Conclusion and Future Work

This chapter is the conclusions and recommendations of the research. It clarifies the researcher's contributions, limitations and future research is suggested.

8.1 The main research contributions

This research, through data derived from grounded theory data collection and data analysis methods, has identified core categories that, when framed within the context of developing and managing a DFO, point toward a framework for building and managing DFC. The research also identified gaps in the literature on how to build and manage a DFO. This is not surprising when the focus in the DF field has been on the investigation process. Yet, both data and literature point to a need for creating a framework that could guide DF experts and managers on how to build and manage a DFO. The existing guidelines such as those from ACPO, though one of the most comprehensive guidelines, remains to be developed further, as recognised by interviewees, partly because it does not look at DF holistically at the organisational level.

The thesis, in Chapter 3, justified the choice for using grounded theory. The choice of grounded theory, in hindsight, was the correct one, mainly because DF is an emerging field, fitting well into Charmaz's (2006) discussion on the strengths of DF in theory building. As Fernandez (2004) observed, grounded theory is well suited in information technology research that involve social interactions between people using information technology or people's interactions with information technology. Since DF is a new field of study, involving interactions between people and technology, grounded theory is most appropriate in developing a framework for DFC (Hewling, 2013; Kessler, 2010; Carlton, 2007). The systematic application of grounded theory in this research as explained in chapters 4 and 5 gives the data strength. As stated in Chapter 5, the systematic application of the coding processes by the researcher is what makes the methodology Straussian, in its approach to grounded theory. The application of this methodology resulted in a set of findings about the data that were separated into categories and core categories as explained in Chapter 6. An understanding of the categories and core categories as they relate and interconnect is

essential to having a better view of how the literature and data support the researcher's proposed theory on DFC.

The work presented in Chapter 7 proposed the DFOCC framework and this is grounded in the data. Chapter 7 also describes the DFOCC framework and how it can be expressed as equations that show the relationships between the four core capabilities, allowing for a proposed definition of DF capability. The DFOCC framework is grounded in the data as a theory which describes the abstract concepts of the core categories. Primarily, the DFOCC framework is related to other theories in the field on DF capability. Consequently, the DFOCC framework has been theoretically combined with other theories, not only by explaining where the DFOCC may fill the gaps in the theories but also where the DFOCC framework can extend the existing models like the capability maturity model and the DFMF.

This research contributes to knowledge:

1. Providing data on how digital forensic organisations build and manage a DF laboratory and organisation.
2. Applying grounded theory to DF research and contributes to knowledge by giving a systematic guidance on how to apply Straussian grounded theory to DF research.
3. Contributing to the knowledge because of the theory that arises from applying grounded theory, which ultimately results in a proposed framework for the developing and managing of a DFC. The core categories that arose from the grounded theory methodology contribute to the knowledge by identifying the core factors that organisations must take into account when building and managing a DFC.
4. Contributing to the knowledge by identifying gaps in the literature on developing and managing a DFC, and proposing the framework as a comprehensive tool for assessing an organisation's needs in developing and managing a DFC.
5. Contributes to knowledge by providing a tool to apply the framework in reality (ch. Section 7.2.2.1) in essence**,** this research has generated a framework for assessing an

organisation's needs in developing and managing a DFC. Also develop a tool to apply the framework in real life (ch. Section 7.2.2.1) and use of the framework and the tool to establish a tool testing capability to prove the applicability of the framework as presented in Appendix 7.

8.2 Research Limitations

Due to time constraint and limited access, any research can face a variety of limitations. For this research, the limitations are that it did not consider the impact of using DFOCC in real life in absence of one or more of the core categories of building DFC. It also did not include a scoring scheme for building the capabilities of the any organisation.

8.3 Future Work

Further work is necessary to extend the testing of the proposed DFOCC with more data, for example, measuring the impact of not having one of the core categories when building capability. Also adding a scoring scheme in the DFOCC software in order to generate a score for an organisation capability. Furthermore, future work would be to aim at creating a universally approved standard, for developing and managing a DFO; and to examine whether it is possible to impose minimum requirements for such factors as the qualifications of DF experts.

There are already ongoing discussions on a minimum educational qualification for DF experts. Data driven research is needed to arrive at reasonable conclusions. Questions remain as to whether a minimum software or hardware set of tools should be available and whether a set of policies must be in place before one can conducts a digital forensic investigation.

References:

Abdelbaqi, M., (2016). Enacting Cybercrime Legislation in an Endeavour to Counter Cybercrime in Palestine. *Global Journal of Comparative Law*, *5*(2), pp.226-261

Accees Data, (2016) available at (http://www.accessdata.com) last accessed on 10/05/2016

ACPO (2012): Association of Chief Police Officers Good Practice Guide for Digital Evidence. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

ACPO Managers Guide (2011): Good Practice ad Advice Guide for Managers of e-Crime Investigation. Version 1.4. http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf.

Ademu, I.O., Imafidon, C.O. and Preston, D.S., (2011). A new approach of digital forensic model for digital forensic investigation. *Int. J. Adv. Comput. Sci. Appl*, *2*(12), pp.175-178

Agarwal, A., Gupta, M., Gupta, S. and Gupta, S.C., (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), pp.118-131

Al Fahdi, M., Clarke, N.L., Li, F. and Furnell, S.M., (2016). A suspect-oriented intelligent and automated computer forensic analysis. *Digital Investigation*,*18*, pp.65-76

Al Obaidli, H. and Iqbal, A., (2011), December. *Digital forensics education in UAE*. In *ICITST* (pp. 766-770)

Alkhateeb, S., (2016) *Cyber Crimes*. International Journal of Scientific & Engineering Research, Volume 7, Issue 4, April-2016 918 ISSN 2229-5518

Allan, G. (2003) *A critique of using grounded theory as a research method.* Electronic Journal of Business Research Methods, 2 (1), pp. 1-10.

Almarzooqi, A. and Jones, A., (2016) January. A Framework for Assessing the Core Capabilities of a Digital Forensic Organization. In *IFIP International Conference on Digital Forensics* (pp. 47-65). Springer International Publishing

Alqahtany, S., Clarke, N., Furnell, S. and Reich, C., (2016). A forensic acquisition and analysis system for IaaS. *Cluster Computing*, *19*(1), pp.439-453

American University in the Emirates (2016) About American University in the Emirates, Available at: [http://www.aue.ae/en/about-aue.html] last accessed on 29-10-2016.

ASCLD, American Society of Crime Lab Directors. (2016). "Accreditation Standards", Available at: http://www.ascld-lab.org/accreditation-standards/. Last Accessed 25-10-2016

Athena Labs (2016) Company Overview, Available at: [https://www.linkedin.com/company/athena-labs] last accessed on 29-10-2016.

Bankole, F., (2013). Proposing a maturity assessment model based on the digital forensic readiness commonalities framework. Master Thesis. The University of the Western Cape

Bariki, H., Hashmi, M. and Baggili, I., (2011). Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools. *Digital Forensics and Cyber Crime*, pp.78-95

Baryamureeba, V. and Tushabe, F., (2004), August. The enhanced digital investigation process model. In *Proceedings of the Fourth Digital Forensic Research Workshop* (pp. 1-9)

Bevan, N., (2001). International standards for HCI and usability. *International journal of human-computer studies*, *55*(4), pp.533-552

Bhosale, D.V., Mitkal, P.K., Pawar, R.N. and Paranjape, R.S., (2016). Review on Computer Forensic. *Training*, *2*(01)

Bidgoli, H.(2006) " Handbook of Information Security,Threats, Vulnerabilities, Prevention, Detection, and Management" Wiley (January 3, 2006)

Birk, D. and Wegener, C., (2011), May. Technical issues of forensic investigations in cloud computing environments. In *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on* (pp. 1-10). IEEE.

Birk, D., (2011), January. Technical challenges of forensic investigations in cloud computing environments. In *workshop on cryptography and security in clouds* (pp. 1-6)

Birks, M. and Mills, J., (2011). *Grounded theory: A practical guide*. Sage publications

Boniface, K.A., Michael, K.A. and Victor, K.O., (2015). *Cyber Security in Nigeria: A Collaboration between Communities and Professionals*. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9(5), pp.1189-1193.

Brenner, S.W. and Schwerha IV, J.J., (2004). Introduction—cybercrime: a note on international issues. *Information Systems Frontiers*, *6*(2), pp.111-114

Brill, A. E., Pollitt, M., & Morgan Whitcomb, C. (2006). The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice, 1(1), 3-11

Brinson, A., Robinson, A. and Rogers, M., (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital investigation*, *3*, pp.37-43.

Bryant, R. ed., (2016). *Policing digital crime*. Routledge

Bryman, A. (2008) *Social research methods*. 3rd ed. Oxford: University of Oxford.

Bukhari, S., Yusof, I. and Abdullah, M.F.A., (2010). Performance evaluation of open-source disk imaging tools for collecting digital evidence. In *Proceedings of Regional Conference on Knowledge Integration in ICT* (p. 353).

Campbell, J.P., Daft, R.L. and Hulin, C.L., (1982). *What to study: Generating and developing research questions* (Vol. 6). Sage Publications, Inc.

Carlton, G. H. (2006). A protocol for the forensic data acquisition of personal computer workstations. Doctoral dissertation, University of Hawaii, Honolulu.

Carlton, G.H., (2007). A grounded theory approach to identifying and measuring forensic data acquisition tasks. *Journal of Digital Forensics, Security and Law*, *2*(1), pp.35-56

Carrier, B. (2002). Open source digital forensics tools: The legal argument. Stake.

Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. digital investigation, 3, 121-130

Casey, E. (2009). Handbook of digital forensics and investigation. Academic Press.

Casey, E. (2011). A unified voice: The need for an international digital forensic convention. Digital Investigation, 8(2), 89-91.

Casey, E. (2012). Editorial: IT security is not enough. Digital Investigation, 9(1),

Casey, E., (2016). Editorial–A sea change in digital forensics and incident response. *Digital Investigation*, *17*, pp.A1-A2

Charmaz, K. (2000). Grounded theory: Objectivist and constructivist methods. In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (2nd ed., pp. 509-535). Thousand Oaks, CA: Sage.

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis. Thousand Oaks, CA: Sage.

Cheek, J. (2000). An untold story: Doing funded qualitative research. In Handbook for qualitative research, 2nd ed., ed. N. Denzin and Y. Lincoln, 401–20. Thousand Oaks, CA: Sage.

Chen, W. and Hirschheim, R., (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information systems journal*, *14*(3), pp.197-235

Choudrie, J. and Dwivedi, Y.K., (2005). Investigating the research approaches for examining technology adoption issues. *Journal of Research Practice*, *1*(1), p.1-12.

Chua, W.F., (1986). Radical developments in accounting thought. *Accounting review*, pp.601-632.

Ciardhuáin, S.Ó., (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), pp.1-22.

Cole, K.A., Gupta, S., Gurugubelli, D. and Rogers, M.K., (2015), January. A Review of Recent Case Law Related to Digital Forensics: The Current Issues. In *Proceedings of the Conference on Digital Forensics, Security and Law* (p. 95). Association of Digital Forensics, Security and Law.

Coleman, C. (2003). Cyberspace security: Securing cyberspace—new laws and developing strategies. *Computer Law & Security Review*, *19*(2), 131-136

Collis, J. and Hussey, R. (2003) *Business research: A practical guide for undergraduate and postgraduate students*. Basingstoke: Palgrave Macmillan.

Computer Misuse Act (1990). The Government of UK available at : (http://www.legislation.gov.uk/ukpga/1990/18/contents) Last Accessed 19-04-2016

Corbin, J. and Strauss, A. (2008) *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage.

Coulondre, S., (2008). Cyber Forensics. *Cyber Warfare and Cyber Terrorism*

Creswell, J. (1998). Qualitative inquiry and research design: Choosing among five traditions. Thousand Oaks, CA: Sage.

Creswell, J. (2005) *Educational research: planning, conducting, and evaluating quantitative and qualitative research*. 2nd ed. New Jersey: Upper Saddle River.

Creswell, J.W., (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications

Cruz-Cunha, M. (2014) *Handbook of Research on Digital Crime, Cyberspace Security (Advances in Digital Crime, Forensics, and Cyber Terrorism).*

Cunliffe, A.L. and Luhman, J.T., (2012). *Key concepts in organization theory*. Sage

Dahbur, K., and Mohammad, B. (2011). The anti-forensics challenge. In *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications* (p. 14). ACM.3.

Deloitte (2016), About Deloitte .Available at: [https://www2.deloitte.com/uk/en/legal/about-deloitte.html] last accessed on 29-10-2016

Delport, W., Köhn, M. and Olivier, M.S., (2011), August. Isolating a cloud instance for a digital forensic investigation. In *ISSA.*

Denscombe, M. (2007) The Good Research Guide: For Small-scale Social Research. 3rd ed. Buckingham: Open University Press.

Dewald, A., (2015). Characteristic evidence, counter evidence and reconstruction problems in forensic computing. *it-Information Technology*,*57*(6), pp.339-346

Dick, B., (2005). Grounded theory: a thumbnail sketch [On line]. *Beschikbaar op*. Last Accessed on 05-05-2013 at (http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html)

Dykstra, J. and Sherman, A.T., 2011, January. Understanding issues in cloud forensics: two hypothetical case studies. In *Proceedings of the Conference on Digital Forensics, Security and Law* (p. 45). Association of Digital Forensics, Security and Law.

Elyas, M., Ahmad, A., Maynard, S.B. and Lonie, A., (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, *52*, pp.70-89

Erbacher, R.F., Christiansen, K. and Sundberg, A., (2006), June. Visual network forensic techniques and processes. In *1st Annual Symposium on Information Assurance: Intrusion Detection and Prevention* (p. 72)

Evidence Talks (2016) Company Overview Available at: [http://www.evidencetalks.com/index.php/about-us] last accessed on 29-10-2016.

Farrell, P.F., (2009). *A framework for automated digital forensic reporting* (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

FBI, Federal Bureau of Investigation Website. (2015). "The Accreditation Decision", Forensics Science Communications, April 1999, Volume 1, Number 1, (http://www.fbi.gov/about-us/lab/forensic-science communications/fsc/april1999/presley.htm/ascldbro.htm.)Last Accessed : 12-02-2015

Fernandez, W.D., (2004). The grounded theory method and case study data in IS research: issues and design. In *Information Systems Foundations Workshop: Constructing and Criticising* (Vol. 1, pp. 43-59).

Find a Masters [Online] (2010) Available from: www.findamasters.com[accessed 19.10.2016]

Flick, U., (2015). *Introducing research methodology: A beginner's guide to doing a research project*. Sage

Freiling, F. and Schwittay, B.,(2007). A common process model for incident response and digital forensics. *Proceedings of the IMF 2007*.

Furnell, S., (2002). *Cybercrime: Vandalizing the information society*. London: Addison-Wesley.

Furnell, S., (2004). Qualified to help: In search of the skills to ensure security. *Computer Fraud & Security*, *2004*(12), pp.10-14

Gable, G.G., (1994). Integrating case study and survey research methods: an example in information systems. *European journal of information systems*, *3*(2), pp.112-126.

Garfinkel, S., (2010) "*Digital forensics research: The next 10 years*," Digital Investigation, vol. 7, pp. S64–S73,

Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. Digital investigation, 6, S2-S11.

Glaser, B. (1978) *Theoretical Sensitivity: Advances in the methodology of grounded theory*. Mill Valley, CA, USA: The Sociology Press.

Glaser, B. (1992) *Emergence vs. forcing: Basics of grounded theory analysis*. Mill Valley, CA, USA: Sociology Press.

Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative research. New Brunswick, NJ: Aldine Transaction.Leedy & Ormrod, 2010;

González-Rojas, O., Correal, D. and Camargo, M., (2016). ICT capabilities for supporting collaborative work on business processes within the digital content industry. *Computers in Industry*, *80*, pp.16-29

Goodman, M.D. and Brenner, S.W., (2002). Emerging Consensus on Criminal Conduct in Cyberspace, The. *Int'l JL & Info. Tech.*, *10*, p.139.

Goodwin, B (2003) Scotland Yard's Computer Crime Unit is cash-strapped but is still catching the crooks. Computerweekly.com, 12 March 2003. Retrieved from: http://www.computerweekly.com (Last Accessed 27-10-2015)

GREAT BRITIAN, Department for International Development, (2015) *National Security Strategy and Strategic Defence and Security Review 2015*. Prime Minister's Office, 10 Downing Street, Cabinet Office, Foreign Commonwealth Office, Home Office, Ministry of Defence. Web version, available on (https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015) Last accessed : 22-04-2016.

Grobler, C. P., & Louwrens, B. (2006). Digital forensics: a multi-dimensional discipline. In *Proceedings of the ISSA 2006 from Insight to Foresight Conference. Pretoria: University of Pretoria*.

Grobler, C. P., Louwrens, C. P., & von Solms, S. H. (2010, February). A framework to guide the implementation of proactive digital forensics in organisations. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 677-682). IEEE

Grobler, C.P., (2011). *A Digital Forensic Management Framework* (Doctoral dissertation, UNIVERSITY OF JOHANNESBURG).

Guest, G, A. Bunce, and L. Johnson (2006) How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. Field Methods, Vol. 18, No. 1, February 2006 59–82. Sage Publications.

Guidance Software, (2016) available at (http://www.guidancesoftware.com) last accessed on 22/10/2016.

Guo, H., Jin, B. and Shang, T., (2012), August. Forensic investigations in cloud environments. In *Computer Science and Information Processing (CSIP), 2012 International Conference on* (pp. 248-251). IEEE.

Guo, Y., Slay, J., and Beckett, J. (2009). Validation and verification of computer forensic software tools—Searching Function. Digital investigation, 6, S12-S22.

Guo, Z. and Sheffield, J., (2008). A paradigmatic and methodological examination of knowledge management research: 2000 to 2004. *Decision Support Systems*, *44*(3), pp.673-688

Haggerty, J. and Taylor, M., (2006). Managing corporate computer forensics. *Computer Fraud & Security*, *2006*(6), pp.14-16

Hales, G., (2016). *Assisting digital forensic analysis via exploratory information visualisation*. Published thesis (PhD), Abertay University.

Hales, G.A., Ferguson, R.I. & Archibald, J.M., (2013). *On the use of hyperbolic visualization to assist digital forensic analysis*. Proceedings of the 3rd International Conference on Cybercrime, Security and Digital Forensics.

Hanaei, A., Hamad, E. and Rashid, A. (2014), May. DF-C2M2: A Capability Maturity Model for Digital Forensics Organisations. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 57-60). IEEE

Harichandran, V.S., Breitinger, F., Baggili, I. and Marrington, A., (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*, *57*, pp.1-13

Hasan, R., Mahmood, S. and Raghav, A., (2012), September. Overview on Computer Forensics tools. In *Control (CONTROL), 2012 UKACC International Conference on* (pp. 400-403). IEEE.

Hegarty, M. Merabti, Q. Shi, and B. Askwith, (2009) "Forensic analysis of distributed data in a service oriented computing platform," in proceedings of the 10th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PG Net,

Hekkala, R. (2007) Grounded theory - the two faces of the methodology and their manifestation in IS research. *Proceedings of the 30th Information Systems Research Seminar in Scandinavia IRIS*, Tampere, Finland, August 11-14, 2007.

Herbst, N.R., Kounev, S., Weber, A. and Groenda, H., (2015), May. BUNGEE: an elasticity benchmark for self-adaptive IaaS cloud environments. In *Proceedings of the 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems* (pp. 46-56). IEEE Press

Hewling, M.O. (2013) 'Digital forensics: an integrated approach for the investigation of cyber/computer related crimes'. PhD thesis. University of Bedfordshire.

Hibshi, H., Vidas, T. and Cranor, L., (2011), May. Usability of forensics tools: a user study. In *IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on* (pp. 81-91). IEEE

High Technology Crime Investigation Association (HTCIA), (2016). Available at: https://www.htcia.org/about/. Last Accessed 22-10-2016

High-Tech Crime Network (HTCN), (2016) Available at: http://www.htcn.org/index.html Last Accessed 22-10-2016

Holt, T.J., (2003). Examining a transnational problem: An analysis of computer crime victimization in eight countries from 1999 to 2001. *International Journal of Comparative and Applied Criminal Justice*, *27*(2), pp.199-220.

Information Technology Act (ITA), (2000) India. Available at (https://eprocure.gov.in/cppp/sites/default/files/itact_contents/IT_DOC_NO_2/itact2000.pdf) last accessed in 26-10-2016.

International Association of Computer Investigation Specialists (IACIS), (2016) available at (https://www.iacis.com) last accessed on 19/10/2016.

Iqbal, A., Obaidli, H.A., Said, H. and Guimaraes, M., (2013) October. The Study of the Interrelation between Law Programs and Digital Forensics in UAE Academia. In *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference* (p. 100). ACM

Islam, M. and Rahaman, M., (2016). A Review on Multiple Survey Report of Cloud Adoption and its Major Barriers in the Perspective of Bangladesh. *International Journal of Computer Network & Information Security, 8*(5)

Jones, A. and Valli, C., (2011). *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility*. Butterworth-Heinemann.

Jones, M. and Alony, I., 2011. Guiding the use of Grounded Theory in Doctoral studies–an example from the Australian film industry

Jones, M.R. and Karsten, H., (2009). Divided by a common language? A response to Marshall Scott Poole. *MIS Quarterly*, pp.589-595

Karyda, M. and Mitrou, L., 2007, August. Internet forensics: legal and technical issues. In *IEEE Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*.

Kaspersky (2016) Company Overview, Available at: [https://www.kaspersky.co.uk/about] last accessed on 29-10-2016.

Kellermann, T. (2010). Building a Foundation for Global Cybercrime law Enforcement. *Computer Fraud and Security,* May, 5.

Kerrigan, M., (2013). A capability maturity model for digital investigations. *Digital Investigation, 10*(1), pp.19-33.

Kessler, G.C., (2010). *Judges' awareness, understanding, and application of digital evidence*. Doctoral Dissertation, Nova Southeastern University.

Khajeh-Hosseini, A., Greenwood, D. and Sommerville, I., (2010), July. Cloud migration: a case study of migrating an enterprise IT system to IaaS. In*Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 450-457). IEEE

Khan, Mohd. (2016)."Cyber Laws in India: The Information Technology Act 2008."*International Journal of Multidisciplinary Approach & Studies* 3, no. 3.

Krutz, R., Krutz Ronald L, (2004). *Methodology for assessing the maturity and capability of an organization's computer forensics processes*. U.S. Patent Application 10/952,537

Lægaard, J. and Bindslev, M., 2006. Organizational theory. *online] Ventus Publishing ApS (BookBoon. com). Available at: (http://fbemoodle.emu.edu.tr/file.php/777/organizational-theory.pdf) Last accessed : 26-04-2016*

Lallie, H.S., 2012. An overview of the digital forensic investigation infrastructure of India. *Digital Investigation*, *9*(1), pp.3-7.

Lang, A., Bashir, M., Campbell, R. and DeStefano, L., (2014). Developing a new digital forensics curriculum. *Digital Investigation, 11*, pp.S76-S84.

Lemieux, F., (2015). Trends in Cyber Operations: An Introduction. In *Current and Emerging Trends in Cyber Operations* (pp. 1-15). Palgrave Macmillan UK.

Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M., (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *arXiv preprint arXiv: 1604.03850*.

Liu, J., & Uehara, T. (2009, March). *Computer forensics in Japan: a preliminary study.* In Availability, Reliability and Security, 2009. ARES'09. International Conference on (pp. 1006-1011). IEEE.

Liu, J., (2016), September. Ten-Year Synthesis Review: A Baccalaureate Program in Computer Forensics. In *Proceedings of the 17th Annual Conference on Information Technology Education* (pp. 121-126). ACM.

Lord, B, (2016) "*An Important Message about Yahoo User Security*". Yahoo. Available (https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security)

Losavio, M., Seigfried-Spellar, K.C. and Sloan III, J.J., (2016). Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies*, *29*(2), pp.143-162

Lyle, J.R., White, D.R. and Ayers, R.P., (2008). Digital forensics at the National Institute of Standards and Technology. *National Institute of Standards and Technology, Interagency Report (NISTIR), 7490*.

Macewan, N.F., (2008). The Computer Misuse Act 1990: lessons from its past and predictions for its future. *Criminal Law Review*, *12*, pp.955-967

Mandiant (2016) Company Overview, Available at: [https://www.fireeye.com/company.html] last Accessed on 29-10-2016.

Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M. and Treichelt, J., (2007) , January. Is the open way a better way? Digital forensics using open source tools. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 266b-266b). IEEE

Marion, N.E., 2010. The council of Europe's cyber crime treaty: An exercise in symbolic legislation. *International Journal of Cyber Criminology*, *4*(1/2), p.699

Marshall, C. and Rossman, G. (1999). Designing qualitative research. Sage Publications.

Marshall, C. and Rossman, G. (2006) Designing qualitative research. 4th ed. Thousand Oaks: Sage.

Martin, P.Y. and Turner, B.A., (1986). Grounded theory and organizational research. *The Journal of Applied Behavioral Science*, *22*(2), pp.141-157

Mason, M., (2010), August. Sample size and saturation in PhD studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research* (Vol. 11, No. 3)

Masood, R., Maqsood, M., Mustaqeem, A. and Azam, M.A., (2016). Cloud Forensics: A Discussion on Open Problems and State-of-the-Art Approaches. *Proceedings Appeared on IOARP Digital Library*.

McAfee (2016), About Us .Available at: [http://www.mcafee.com/us/index.html] last accessed on 29-10-2016.

McAuley, J., Duberley, J. and Johnson, P., (2007). *Organization theory: Challenges and perspectives*. Pearson Education.

McCarrin, M. and Garfinkel, S.L., 2014. Challenges to Consensus and Consistency in DF Education. Monterey, California. Naval Postgraduate School

McEvoy, P. and Richards, D., (2006). A critical realist rationale for using a combination of quantitative and qualitative methods. *Journal of Research in Nursing*, *11*(1), pp.66-78

Mell, P. and Grance, T., (2010). The NIST definition of cloud computing. *Communications of the ACM*, *53*(6), p.50.

Meyers, M. and Rogers, M., (2004). Computer forensics: the need for standardization and certification. *International Journal of Digital Evidence*, *3*(2), pp.1-11.

Miles, M., and A. Huberman. (1994). Qualitative data analysis. 2nd ed. Thousand Oaks, CA: Sage.

Montasari, R., (2016). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*,*8*(4), pp.285-302

Montasari, R., (2016). Review and Assessment of the Existing Digital Forensic Investigation Process Models. *International Journal of Computer Applications*, *147*(7)

Montasari, R., Peltola, P. and Carpenter, V., (2016), June. Gauging the effectiveness of computer misuse act in dealing with cybercrimes. In *Cyber Security And Protection Of Digital Services (Cyber Security), 2016 International Conference On* (pp. 1-5). IEEE.

Mouhtaropoulos, A., Grobler, M. and Li, C.T., (2011), September. Digital forensic readiness: an insight into governmental and academic initiatives. In*Intelligence and Security Informatics Conference (EISIC), 2011 European*(pp. 191-196). IEEE

Mouhtaropoulos, A., Li, C.T. and Grobler, M., (2014). Digital Forensic Readiness: Are We There Yet. *J. Int't Com. L. & Tech.*, *9*, p.173

Myers, M.D., (1997). Qualitative research in information systems. *Management Information Systems Quarterly, 21*(2), pp.241-242

Nance, K. and Ryan, D.J., 2011, January. Legal aspects of digital forensics: a research agenda. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-6). IEEE

Nance, K., Armstrong, H., & Armstrong, C. (2010, January). Digital forensics: Defining an education agenda. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* (pp. 1-10). IEEE.

Naqvi, S., Dallons, G. and Ponsard, C., (2010), October. Protecting corporate ICT infrastructures by using digital forensics. In *Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on* (pp. 255-258). IEEE.

National Institute of Justice, U.S. Department of Justice (2010) Digital Forensics Standards and Capacity Building [www.nij.gov] Published on 5 Nov 2010 available:(http://nij.gov/topics/forensics/evidence/digital/standards/welcome.htm) Accessed on 02/07/2012.

National Institute of Standards and Technology (NIST),USA department of Commerce, 2016. Available at (http://www.nist.gov/index.html), last accessed on 19/10/2016.

National Research Council, (2009). Strengthening forensic science in the United States: A path forward.

Neuman, W. (2004) Basic of social research qualitative and quantitative approaches. Boston, MA: Pearson/Allyn and Bacon.

Neuman, W. (2006) Social research methods: qualitative and quantitative approaches. 6th ed. Boston: Pearson.

Neuman, W. (2011) Social research methods: qualitative and quantitative approaches. 7th ed. Boston: Pearson.

Nielsen, J. and Landauer, T.K., 1993, May. A mathematical model of the finding of usability problems. In *Proceedings of the INTERACT'93 and CHI'93 conference on Human factors in computing systems* (pp. 206-213). ACM.

Nikkel, B.J., (2006), May. *The role of digital forensics within a corporate organization.* In May 2006, IBSA Conference, Vienna.

Nuix (2016), About Nuix, Available at: [https://www.nuix.com/about-nuix] last accessed on 29-10-2016.

Nuth, M.S., (2008). Taking advantage of new technologies: For and against crime. *Computer Law & Security Review*, *24*(5), pp.437-446.

O'Brien, R., (1998). An overview of the methodological approach of action research. *Faculty of Information Studies, University of Toronto*.

Oates, B.J. (2006). Researching Information Systems and Computing. Middlesborough UK: Sage Publications Ltd.

O'Leary, Z. (2009). The essential guide to doing your research project. Sage.

O'leary, Z., (2004). *The essential guide to doing research*. Sage.

Orlikowski, W.J. and Baroudi, J.J., (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, *2*(1), pp.1-28

Orlikowski, W.J., (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS quarterly*, pp.309-340.

Palmer, G., (2001), August. A road map for digital forensic research. In *First Digital Forensic Research Workshop, Utica, New York* (pp. 27-30)

Parsons, T. and Jones, I., (1960). *Structure and process in modern societies* (Vol. 3). New York: Free Press

Paul, M., (2012). Business leaders urged to step-up response to cyber threats| News| BIS. available At: (https://www.gov.uk/government/news/business-leaders-urged-to-step-up-response-to-cyber-threats) Last accessed on the :01/04/2016

Paulk, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V., (1993). Capability maturity model, version 1.1. *IEEE software*, 10(4), pp.18-27

Perumal, S., (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, *9*(8), pp.38-44.

Phillips, A. and Nance, K.L., (2010), May. Computer Forensics Investigators or Private Investigators: Who Is Investigating the Drive?. In *Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on* (pp. 150-157). IEEE

Pickard, A. J., & Childs, S. (2007). *Research methods in information*. London: Facet.

Pogson, C.E., Bott, J.P., Ramakrishnan, M. and Levy, P.E., (2002). A grounded theory approach to construct validity: Investigating first-order constructs in organizational justice to triangulate with current empirical research. In *Research Methods Forum* (Vol. 7).

Poisel, R. and Tjoa, S.,(2011), May. Forensics investigations of multimedia data: A review of the state-of-the-art. In *IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on* (pp. 48-61). IEEE

Pollitt, M., (1995), October. Computer forensics: An approach to evidence in cyberspace. In *Proceedings of the National Information Systems Security Conference* (Vol. 2, pp. 487-491).

Pollitt, M.M., (2001), October. Report on digital evidence. In *13th INTERPOL Forensic Science Symposium*.

Pollitt, M.M., (2007), April. An ad hoc review of digital forensic models. In *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on* (pp. 43-54). IEEE.

Poonia, A.S., Banerjee, C. and Banerjee, A., (2016). Improvised Cyber Crime Investigation Model. In *Proceedings of Fifth International Conference on Soft Computing for Problem Solving* (pp. 743-751). Springer Singapore

Preeti Kannan (2011) Cyber crime hits '76% of residents. The National on the 04/10/2011. Available on (http://www.thenational.ae) last accessed on (26- 10- 2015)

Price Waterhouse Coopers (PwC) (2016) *Adjusting the Lens on Economic Crime Preparation brings opportunity back into focus*. Global Economic Crime Survey 2016:

Available at: (https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf) Last Accessed:03/10/2016

Rani, D.R., Sultana, S.N. and Sravani, P.L., (2016). Challenges of Digital Forensics in Cloud Computing Environment. *Indian Journal of Science and Technology*, *9*(17)

Reddy, K. and Venter, H.S., (2013). The architecture of a digital forensic readiness management system. *Computers & Security*, *32*, pp.73-89

Reilly, D., Wren, C. and Berry, T., (2011). Cloud computing: Pros and cons for computer forensic investigations. *International Journal Multimedia and Image Processing (IJMIP)*, *1*(1), pp.26-34.

Reith, M., Carr, C., & Gunsch, G.(2002), "An examination of digital forensic models," International Journal of Digital Evidence, vol. 1, no. 3, pp. 1–12, 2002.

Remenyi, D. and Williams, B., (1998). *Doing research in business and management: an introduction to process and method*. Sage

Richardson, R. and Director, C.S.I., 2008. CSI computer crime and security survey. *Computer Security Institute*, *1*, pp.1-30

Robson, C. (2002) Real World Research. Oxford: Blackwell

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2*(3), 1-28.

Rowlingson, R., (2005). An introduction to forensic readiness planning. *Centre for the Protection of National Infrastructure (CPNI)*, *27*

Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M., 2011, January. Cloud forensics. In *IFIP International Conference on Digital Forensics* (pp. 35-46). Springer Berlin Heidelberg

Sabeil, E., Manaf, A.A. and Ismail, Z., (2011). Analysing the Quality Assurance of Trainees Competency Assessment and Accreditation of Cyber Forensic Education/Training Programs. ICMLC.

Saleem, S., 2015. Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics.

Sanad, A.A., (2012). Developing an Integrated Model to Support Effective Customer Relationships Management Implementation within the Private Sector of the Kingdom of Saudi Arabia. PhD Thesis, De Montfort University.

Saunders, M. Lewis, P. and Thornhill, A. (2003) *Research methods for business students*. London: Prentice Hall.

Schein, E. (1970) Organizational Psychology, 2nd edn, Englewood Cliffs, NJ: Prentice-Hall.

Schell, B.H. and Martin, C., (2004). *Cybercrime: A reference handbook*. ABC-CLIO

Sekaran, U., (2006). *Research methods for business: A skill building approach*. John Wiley & Sons.

Shapiro, A. (1999). The Internet. *Foreign Policy*, 115, 14-27.

Shrivastava, G., Sharma, K. and Dwivedi, A., (2012). Forensic Computing Models: Technical Overview. *CCSEA, SEA, CLOUD, DKMP, CS & IT*, *5*, pp.207-216

Sibiya, M.G., (2015). *Digital Forensic Model for a Cloud Environment* (Doctoral dissertation, University of Pretoria).

Sinangin, D. (2002). Computer forensics investigations in a corporate environment. Computer Fraud & Security, 2002(6), 11-14

Sinrod, E.J. and Reilly, W.P., (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws. *Santa Clara Computer & High Tech. LJ*, *16*, p.177.

Sommer, P. (2010). Forensic science standards in fast-changing environments. *Science & Justice*, *50(1)*, *12-17.*

Sommer, P., (2011). Certification, registration and assessment of digital forensic experts: The UK experience. *digital investigation*, *8*(2), pp.98-105.

Sommer, P., (2012). Digital evidence, digital investigations and e-disclosure: a guide to forensic readiness for organizations, security advisers and lawyers. *Information Assurance Advisory Council (IAAC)*, pp.1-115

StarLink (2016) Company Overview. Available at: [http://www.starlinkme.net/] last accessed on 29-10-2016

Stemler, S., (2001). An overview of content analysis. *Practical assessment, research & evaluation*, *7*(17), pp.137-146.

Stephenson, P., (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, *8*(2), pp.42-54.

Strauss, A. and Corbin, J. (1990) *Basics of qualitative research: grounded theory procedures and techniques*. Newbury Park, California: Sage.

Strauss, A. and Corbin, J. (1998) *Basics of qualitative research: techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage.

Supreme Court of the United States, (1993). Daubert v. Merrell Dow Pharmaceuticals Syllabus. June 28. Available at: http://supct.law.cornell.edu/supct/html/92-102.ZS.html

Taylor, C., Endicott-Popovsky, B. and Frincke, D.A., 2007. Specifying digital forensics: A forensics policy approach. *Digital investigation*, *4*, pp.101-104 (a)

Taylor, C., Endicott-Popovsky, B., & Phillips, A. (2007, April). *Forensics education: Assessment and measures of excellence. In Systematic Approaches to Digital Forensic Engineering,* 2007. SADFE 2007. Second International Workshop on (pp. 155-165). IEEE.(b)

Telecommunication Regulatory Authority (TRA), (2016) About TRA, Available at: [https://www.tra.gov.ae/en/about-tra/about-tra-vision-mission-and-values.aspx] last accessed on 29-10-2016.

The International Society of Forensic Computer Examiners (ISFCE), 2016 Available at (http://www.isfce.com) last accessed on 22/10/2016.

Thornberg, R., and K. Charmaz, (2012). Grounded theory. In *Qualitative research: An introduction to methods and designs*. Edited by S. D. Lapan, M. T. Quartaroli, and F. J. Riemer, 41–67. San Francisco, CA: Jossey-Bass.

UCAS (2016) available at [https://www.ucas.com/] Accessed: 19-10-2016

Urquhart, C., Lehmann, H. and Myers, M.D., (2010). Putting the 'theory'back into grounded theory: guidelines for grounded theory studies in information systems. *Information systems journal*, *20*(4), pp.357-381

Valjarevic, A. and Venter, H.S., (2012), August. Harmonised digital forensic investigation process model. In *2012 Information Security for South Africa*(pp. 1-10). IEEE.

Vanlalsiama, B. and Jha, N., (2015). Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes. *IITM Journal of Management and IT*, *6*(1), pp.123-128

Volonino, L., Anzaldua, R. and Godwin, J., 2006. *Computer Forensics: Principles and Practices (Prentice Hall Security Series)*. Prentice-Hall, Inc.

Von Solms S, Louwrens C, Reekie, C, and Grobler, T. (2006). A control Framework for Digital Forensics in *Advances in Digital Forensics II, IFIP Advances in Information and Communication Volume* 222, 2006, pp 343-355.

Von Solms S, Louwrens C (2005). Relationship between Digital Forensics, corporate Governance, Information Technology and Information Security Governance, Information Security of South Africa Conference 2005 proceeding.

Von Solms, B., (2001). Information security—a multidimensional discipline. *Computers & Security*, *20*(6), pp.504-508.

Walden, I. (2004). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice, 12*(4), 321-336.

Walsham, G. (1995) *Interpretive case studies in IS research: nature and method.* European Journal of Information Systems, 4(2), pp. 74–81.

Wang, S. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crimes, *Computer Standards and Interfaces*, 29, 216-223.

Watson, D.L. and Jones, A., (2013). *Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements*. Newnes

Wazid, M., Katal, A., Goudar, R.H. and Rao, S., (2013), April. Hacktivism trends, digital forensic tools and challenges: A survey. In *Information & Communication Technologies (ICT), 2013 IEEE Conference on* (pp. 138-144). IEEE.

West Yorkshire Police (2016), About Us, Available at: [https://www.westyorkshire.police.uk/about-us] last accessed on 29-10-2016.

Whitcomb, C.M., (2002). An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, *1*(1), pp.5-9.

Wilson, J., (2010). *Essentials of Business Research: A Guide to Doing Your Research Project*. SAGE Publications.

Wolthusen, S.D., (2009), September. Overcast: Forensic discovery in cloud environments. In *IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on* (pp. 3-9). IEEE

Yasinsac, A. and Manzano, Y., (2001), June. Policies to enhance computer and network forensics. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security* (pp. 289-295)

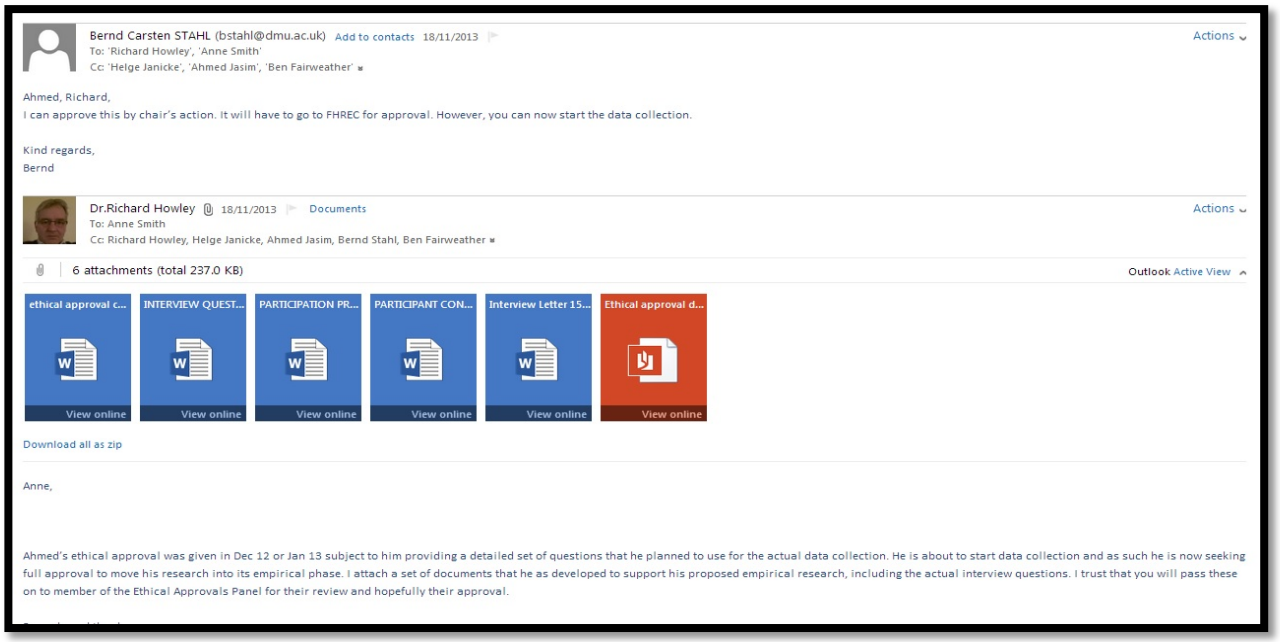
Yates, S., (2003). *Doing social science research*. Sage.

Yin, R. (2009) *Case study research: design and methods.* 4th ed. Thousand Oaks: Sage.

Zawoad, S. and Hasan, R., (2013). Cloud forensics: a meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv:1302.6312*

Appendices

APPENDIX 1: Email Confirmation of the ethical approval



Bernd Carsten STAHL (bstahl@dmu.ac.uk) Add to contacts 18/11/2013 Actions

To: 'Richard Howley', 'Anne Smith'
Cc: 'Helge Janicke', 'Ahmed Jasim', 'Ben Fairweather'

Ahmed, Richard,
I can approve this by chair's action. It will have to go to FHREC for approval. However, you can now start the data collection.

Kind regards,
Bernd

Dr.Richard Howley 18/11/2013 Documents Actions

To: Anne Smith
Cc: Richard Howley, Helge Janicke, Ahmed Jasim, Bernd Stahl, Ben Fairweather

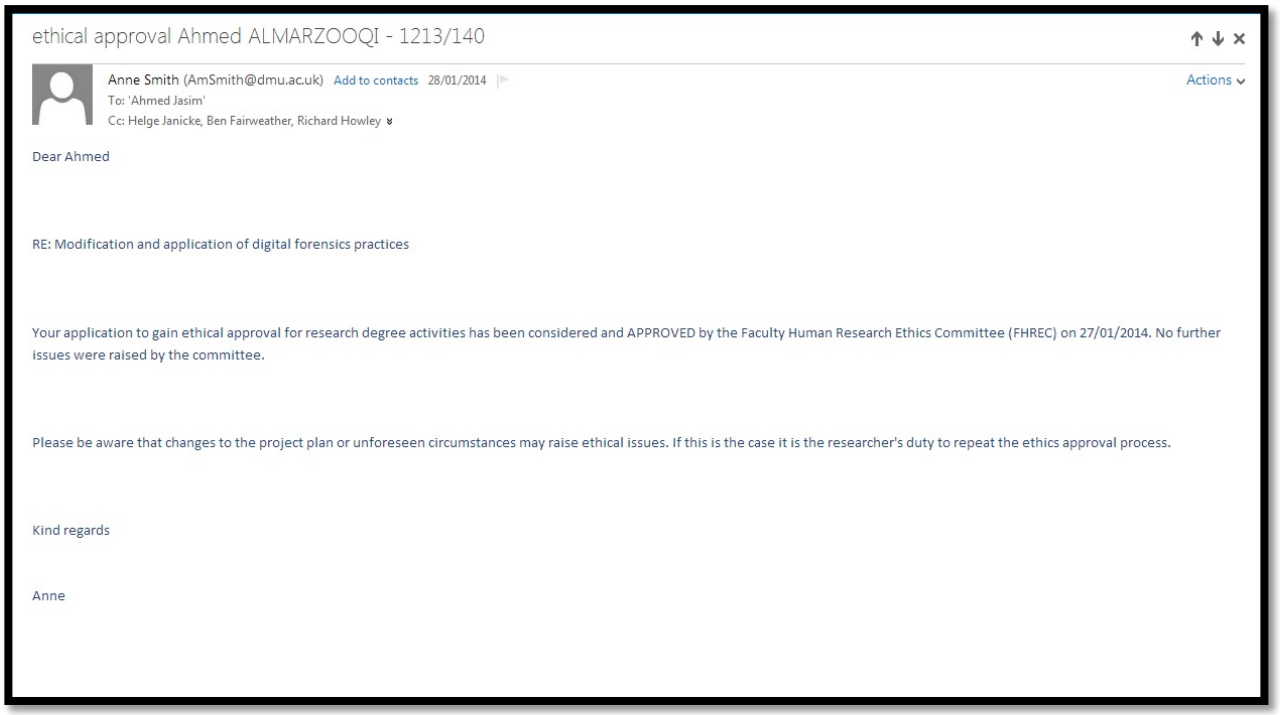
6 attachments (total 237.0 KB) Outlook Active View

ethical approval c... View online | INTERVIEW QUEST... View online | PARTICIPATION PR... View online | PARTICIPANT CON... View online | Interview Letter 15... View online | Ethical approval d... View online

Download all as zip

Anne,

Ahmed's ethical approval was given in Dec 12 or Jan 13 subject to him providing a detailed set of questions that he planned to use for the actual data collection. He is about to start data collection and as such he is now seeking full approval to move his research into its empirical phase. I attach a set of documents that he as developed to support his proposed empirical research, including the actual interview questions. I trust that you will pass these on to member of the Ethical Approvals Panel for their review and hopefully their approval.



ethical approval Ahmed ALMARZOOQI - 1213/140

Anne Smith (AmSmith@dmu.ac.uk) Add to contacts 28/01/2014 Actions

To: 'Ahmed Jasim'
Cc: Helge Janicke, Ben Fairweather, Richard Howley

Dear Ahmed

RE: Modification and application of digital forensics practices

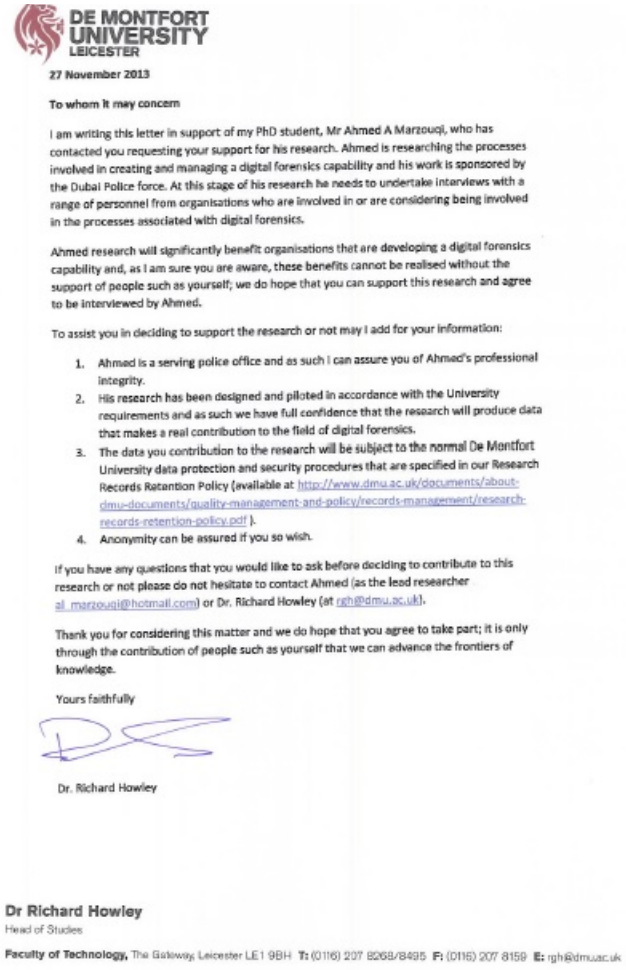
Your application to gain ethical approval for research degree activities has been considered and APPROVED by the Faculty Human Research Ethics Committee (FHREC) on 27/01/2014. No further issues were raised by the committee.

Please be aware that changes to the project plan or unforeseen circumstances may raise ethical issues. If this is the case it is the researcher's duty to repeat the ethics approval process.

Kind regards

Anne

APPENDIX 2: Letter from supervisor regarding research



DE MONTFORT UNIVERSITY LEICESTER

27 November 2013

To whom it may concern

I am writing this letter in support of my PhD student, Mr Ahmed A Marzouqi, who has contacted you requesting your support for his research. Ahmed is researching the processes involved in creating and managing a digital forensics capability and his work is sponsored by the Dubai Police force. At this stage of his research he needs to undertake interviews with a range of personnel from organisations who are involved in or are considering being involved in the processes associated with digital forensics.

Ahmed research will significantly benefit organisations that are developing a digital forensics capability and, as I am sure you are aware, these benefits cannot be realised without the support of people such as yourself; we do hope that you can support this research and agree to be interviewed by Ahmed.

To assist you in deciding to support the research or not may I add for your information:

1. Ahmed is a serving police office and as such I can assure you of Ahmed's professional integrity.
2. His research has been designed and piloted in accordance with the University requirements and as such we have full confidence that the research will produce data that makes a real contribution to the field of digital forensics.
3. The data you contribution to the research will be subject to the normal De Montfort University data protection and security procedures that are specified in our Research Records Retention Policy (available at http://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/records-management/research-records-retention-policy.pdf).
4. Anonymity can be assured if you so wish.

If you have any questions that you would like to ask before deciding to contribute to this research or not please do not hesitate to contact Ahmed (as the lead researcher al_marzouqi@hotmail.com) or Dr. Richard Howley (at rgh@dmu.ac.uk).

Thank you for considering this matter and we do hope that you agree to take part; it is only through the contribution of people such as yourself that we can advance the frontiers of knowledge.

Yours faithfully

Dr. Richard Howley

Dr Richard Howley
Head of Studies
Faculty of Technology, The Gateway, Leicester LE1 9BH **T:** (0116) 207 8268/8495 **F:** (0116) 207 8159 **E:** rgh@dmu.ac.uk

APPENDIX 3: Interview Protocol and Questions

1- Purpose of the Interview:

Identify patterns in establishing and managing digital forensics organisations with the ultimate aim of proposing a development framework for establishing and managing Digital Forensics Capability.

2- General Information about the Interview

Participant Name:	Organisation:	Role in the Organisation:
Place of the Interview:	Date of the Interview:	Duration of the Interview:
Language interview conducted :	Electronic Copy: YES / NO	

3- Interview check list:

- Introduce yourself + Shake hands + Exchange business cards
- Inform the participant about the purpose of the interview
- Show the participant letter from the University declaring the data is collected for research purposes
- Ask the participant permission to record the interview with a digital recorder and taking notes during the interview
- Inform the participant about the stages of the interview (Sections = 5 , No. of questions = 30 and duration = 60 minutes)
- Give the participant consent form
- Ask the participant if he has any questions

- Start the questions and start the timer
- At the end of the interview the researcher will summarise the interview session and thank the participant ask to contact you if he has more clarification regarding his answers

3- INTERVIEW QUESTIONS

A - Background Questions:

4. How long you have been in the field of Digital Forensics (DF)?
5. How long you have been in this organisation?
6. What is your field of study? (qualification)

B- Research Questions:

	Question	Purpose	Expected answer
1-Guidelines and Procedures (1-10)			
1.	Do you know of any guidelines for developing a DFO or DF provision?	To determine if there is a guideline for developing DFO	No ,only available text book for building a managing a successful laboratory does not provide a framework but follows an informal list of factors for what the author believe what successful lab is
2.	Do you know any guideline for managing DF provision and or DFOs?	To determine if there is a guideline for managing a DFO	No ,only available text book for building a managing a successful laboratory does not provide a framework but follows an informal list of factors for what the author believe what successful lab is
3.	If there if is a guideline please provide the name or source?	To determine if there is a guideline for developing or managing a DFO, which is the research problem?	None
4.	Do you follow any such	To see how widely guidelines	No ... if they know of

guideline?	are used	guidelines and they don't follow them – explore why.
5. How did you establish your DF provision/organisation? Can you identify steps taken to develop your DFO or facility?	To determine or identify pattern that DFO use in developing DFO	-Establish key HR positions -Purchase key hardware and software -Develop key policies to govern access to facilities
6. How do you define an organisation to be digital forensically capable?	To determine how DF orgs define a DF capable org	-After successfully investigating a case
7. What is the digital capability of your company?	To determine how DF orgs define a DF capable org	The ability to investigate in crimes involves the use of media devices
8. What is the key factor to your business or your success?	To determine how DFOs define a DF capable organisation	Training , keeping up-to-date with latest technology and experience
9. What minimum factors must be present for a DFO to be considered capable of DF investigation?	To determine what DFOs see as minimum requirements for DF capacity	-Available tools and ability of DF investigator
10. What do you see is the biggest challenge or obstacle in developing DF capability initially when you started?	To identify patterns that DF investigators and managers see as obstacles	Technology , Training

2-Infrastructure (11-16)

11. What are you commonly used tools in DF lab (Hardware and Software) • What is the reason behind using this particular software? • Is this due to business requirement? • Is it because of the efficiency of these products? • Or is it for financial reasons? • Do you consider using open source tools and why?	To identify a standard pattern for DF capability, process and tools in private or public organisations To identify the reason behind choosing specific tool or software To see how widely free tools are used and reliable	According to the crimes, situation or scenario which requires investigation. EnCase and FTK could be the strongest candidates. According to the business need and finical capability Yes to verify investigation results
12. What are extra 'accessories' or tools i.e. Portable devices for mobile investigation you would like to have in a DF laboratory)?	To determine how DFO sees infrastructure capacity	Sufficient software and hardware
13. Do you use cloud environment? If yes – for what purpose do you use it? i.e. 14. Do you use for storage? 15. Do you use it as platform for software? Why do you use cloud? If no, why not? Any future plans for cloud?	To determine if cloud computing is used	No, maybe they use cloud for personal concerns
16. Do you think laboratory accreditation by ISO standard is important/ beneficial? Why? i.e. ISO17025 for mobile phone laboratory accreditation	To determine if ISO Certification is a minimum requirement for DF infrastructure capability	Yes, and we follow the ISO Standards for investigation but not for the DFO

3-Organisational Polices (17-20)		
17. Do you have any policy in place governing people in Labs?? I.e. the use of smart phones, memory sticks in laboratories **why**?	To identify a standard pattern for DF capability polices in private or public organisations	No
18. If 17 is yes then - Is there a: - Conflict of interest policy? or - Confidentiality policy?	To determine to what extent the DF org prevents security breaches that stems from personnel	No
19. Do you think having polices contribute to the capability of a DFO?	To distinguish the role of DF readiness from DF capacity and to determine the impact of DF readiness on DF capacity	DF readiness makes the prediction of DF capacity requirements more predictable
20. What policies do you have in place to organise the use of internet in the investigation environment	To determine what types of policies are in place to prevent security breaches	Chain of evidence policy
4- Human Resources (21-26)		
21. How are you Organised? I.e. Manager, lab staff, investigators.	To find out the management structure and the use of organisation theory applied in creating and managing DFC	Overview of department structure will vary
22. How authority is exercised? Do you have a choice to do what you like?	To find out the management structure and the use of organisation theory applied in creating and managing DFC	Everyone has a clear job description and tasks are assigned according to the availability/ability of the staff for each task
23. What are the key positions that a DFO must have?	To identify a standard pattern for DF capability in private or public organisations	DF investigator
25. How do you become a digital forensic investigator? • Do you require a particular qualification to become a DF	- To determine the minimum requirement/qualification for a DF investigator - To determine if there	- Computer security - The training is based on the business requirement

investigator? • Do you require a particular training for executing DF investigation? • How long experience do I need to become a DF investigator? And is there a particular field to work in?	is particular certification or experience required to become an investigator - To determine if there is a pattern in qualifying a DF investigator	
24. Can you give me the name of a particular qualification that you particularly value?	To determine the minimum requirement of a DF investigator	College degree in field, training and/or experience
25. Do you require your DF Investigators to undergo continuing education workshop/training? If so, how often and up to what level? If not, why not?	To determine whether there is a pattern in training of DF personnel	Yes, It depends on the budget and time.
5- Investigation Process (27-29)		
26. Do you have a documented process for investigation? If yes can you explain or provide me with a source	To identify of there is a standard process to follow in investigations	Yes
27. Are there particular pressures that cause your process any difficulty? Or is there any difficulty in any of the process that causes pressure on the investigator? why	To identify a pattern of pressures from various stakeholders have on investigators during the different stages of a DF investigation	-Lack of time -Technological limitations -Lack of DF readiness -Lack of HR capacity or qualification
28. What areas could the process of the investigation is improved?	To determine how DF capacity could improve DF investigation vulnerabilities	Technological capacity to cover new ways of hiding digital evidence like cloud computing
29. From your experience, what area(s) in the DF Investigation process is most vulnerable to legal challenge? Why?	To determine how DF capacity could improve the success rate of digital evidence admissibility in court	Depends on the case; lack of complete data

At the End of Interview:

Thank the participant and ask if he/she has any final comment that they feel will add value to the research and was not asked by the researcher?

Glossary:

Digital Forensic Organisation: a social unit of people engaged in DF that are structured and managed to meet a need or to pursue collective goals that are related to DF. This organisation can also be referred to the social unit engaged with DF Laboratory

Facility: a place, amenity, or piece of equipment provided for a particular purpose (Oxford Dictionary, 2013)

Capability: the power or ability to do something (Oxford Dictionary, 2013)

Digital Forensic Capability: the ability to establish and manage Digital Forensic Facility with proper staffing, training, selecting tools and providing managerial framework

Guideline: a general rule, principle, or piece of advice: i.e. the organization has issued guidelines for people working with prisoners (Oxford Dictionary, 2013)

Framework: a basic structure underlying a system, concept, or text. i.e. the theoretical framework of political sociology (Oxford Dictionary, 2013)

APPENDIX 4: Participation Procedure and Consent Form

Recruitment

This research focuses on identifying patterns in establishing and managing digital forensics organisations with the ultimate aim of proposing a development framework for establishing and managing Digital Forensics organisation.

The criteria that will be used for selecting the sample are those organisations that engage in digital forensics. A digital forensics investigator, digital forensics manager, digital forensics lab owner or operator, digital forensics director, digital forensics sponsor, law enforcement officers and experts, digital forensics academics, or digital forensics expert to participate in the interview within both private and public sector organisations.

To obtain in-depth and relevant information on the research questions, a series of semi-structured interviews will be conducted, affording the informants the opportunity of supplying their opinions, knowledge and experience on a wide range of issues.

Consent

See document: Consent form for Research Study

Written and Signed Consent of Participants must be obtained prior to the start of any interview. The Interview Sheet will identify with a tick box that a Written and Signed Consent from the Participant has been obtained.

Confidentiality

No personal identification data will be stored. Respondents will be assigned unique respondent number that identifies their data and which can be used to withdraw the data from the study, if necessary. Data will be stored, processed and ultimately destroyed in accordance with the DMU Research Data Retention Policy; The Policy is available at: http://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/records-management/research-records-retention-policy.pdf

Modification and Application of Digital Forensics Practices

CONSENT FORM :

Participant Code: _____

Issue

- I have read the information presented in the information letter about the PhD research being conducted by Mr. Ahmed Almarzooqi at the Faculty of Technology at De Montfort University.

- I have had the opportunity to ask any questions related to this study and have received satisfactory answers to my questions.

- I am also aware that excerpts from the interview may be included in publications resulting from this research. Quotations will/will not be kept anonymous. I do/do not give permission for my identity to be revealed in the research reports.

- I was informed that I may withdraw my consent at any time by advising the researcher. And using my unique respondent code issued to me at the interview'.

- I give permission for the interview to be recorded.

- I understand that data collected during the interview may be looked at by individuals from De Montfort University, where it is relevant to this research. I give permission for these individuals to have access to my responses. It is anticipated that PhD supervisors and examiners may require access to the data collected at interviews.

With full knowledge of the foregoing, I agree to participate in this study.

I agree to being contacted again by the researchers if my responses give rise to interesting findings or cross references. _____ NO ____ YES

If yes, my preferred method of being contacted is:

Telephone ……..

Email …….

Other ……..

Participant Name: Interviewer Name:

Participant Signature:	Interviewer Signature:
Date:	Date:

APPENDIX 5 : Overview and Agreement to Participate in Digital Forensics Research Study Ahmed Almarzooqi, Doctoral Researcher

Dear Participant,

This letter is to give you information in the hope that you will participate in a study about digital forensics in the private and public sectors. I am currently a PhD student in Digital Forensics in the Faculty of Technology at De Montfort University, Leicester, United Kingdom. This research is sponsored by the Dubai Police, Ministry of Interior, United Arab Emirates, where I was last assigned as Head of Quality Assurance Office, Head of Financial Crime Branch, and lastly Head of Administration and Human Resources Section.

The purpose of this research is to study the stages and procedures for establishing and managing digital forensics organisations and capabilites. More specifically, this research aims to identify patterns in digital forensics organisations to ultimately propose a framework for establishing a digital forensic capability. Your participation and valuable contribution will help me:

- Identify, document, and evaluate the stages and procedures for establishing a digital forensics organisation.
- Propose a framework for establishing digital forensics capability.
- Benefit both the academic community and digital forensic practitioners in public and private sector organisations.

I believe that there is little or no risk to participating in this research. All data will be maintained in accoradance with DMU policy, available at: http://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/records-management/research-records-retention-policy.pdf.

If you request, your name or any other personal identifying information will not appear in any publications resulting from this research; neither will there be anything to identify your place of work or business.

Participation in this study is entirely voluntary. You will receive no compensation for participating in this study. It will involve approximately 60 minutes, and at a location agreed upon in advance between you and Mr. Ahmed Almarzooqi.

You may decide not to answer any of the interview questions if you wish. You may also decide to withdraw from this study at any time by advising Mr. Ahmed Almarzooqi. I may ask for clarification after the interview, but you are not obliged in any way to clarify or

participate further. Beyond that I will not seek any more interviews or make any further contact with you about this after the interview without your express consent.

Even though I may present the study findings to Conferences, Journals and Information Society Doctoral Programme Committees, only my supervisors, Dr. Richard Howley and Dr. Helge Janicke, my thesis examiners and I will have access to the interview data itself.

If you have any questions regarding this study or would like additional information please ask me before, during, or after the interview. If you have any questions regarding your rights as a research participant, please contact:

Lead Researcher: **Ahmed Almarzooqi**

Email : **ahmed.almarzooqi@email.dmu.ac.uk**

First Supervisor: **Dr.Richard Howley**

Email: **rgh@dmu.ac.uk**

I can assure you that this research has been reviewed and approved by my supervisors.

Thank you for your assistance in this project.

Best regards,

Ahmed Almarzooqi

APPENDIX 6: Example of Data Analysis

A- Open Coding

Question	Open Codes	02CONINTUAE13	01BLKINTUK13
5- How did you establish your DF provision/organisation? Can you identify steps taken to develop your DFO or facility?	02CONINTUAE13 - Forensic Lab Core module required - Different types of investigation - field of forensic is an ocean because of technology - Make Sure you are able to acquire the potential evidence - Many companies that have come up out of nowhere **01BLKINTUK13** - Studied forensic and security in the university, then disaster recovery, security, then external training and certification and more specialised training then started Looking for a job - No suitable job then decided to have my own company - I set up a limited company - bought my equipment through contacts -I started picking up work for police and law firms - Very difficult to start with and work can be infrequent	we have the core forensics lab, which is basically the basic core modules that are required like for example you need to analyse to basically acquisition, acquiring evidence, evidence acquisition on… and analysis… so evidence preservation… so all these are modules for specific types of forensics, so also you have, as you know, you have different types of investigations. You have e-mail, you have malware analysis now which is a hot thing, internet investigation, network forensics, browser, mobile, Mac. Because of the technology that has come out in the last, I would say, like 15 to 20 years, like especially the last 10 years, I would say. The field of forensics is quite… is an ocean now because you're dealing with different types technologies and you have to make sure that you're capable of acquiring this potential evidence. And basically you're able to acquire it in a way which is obviously [inaudible] with the chain of custody. Now, there are now flourishing in the last few years, I would say, based on my experience, many companies that have come up out of nowhere, specializing in different types of forensics, as you're aware of	Well, when I did my Masters degree, I d it part-time. Okay. And the main forens modules I did very early on. Okay, so th first modules I did were the forensic modules because I did forensic comput and security. So started off with the forensics, then we went through, sort o the…we covered things like disaster an recovery and so on, and then on the security side. So once I've done the ma forensic module, I started getting external training with companies such a Micro Systemation for XRY, getting my certification and so on…. And then I we on, sort of, other training which was in then to specifics, so it may be data carving and so on… getting my certification, my certification in that. An then I started looking at the jobs marke I started looking at working for the police…potentially, and working for oth companies as a forensic examiner. But didn't find anything suitable. And the problem was, effectively, I was class…I' have to go like the graduate scheme an because I was over forty… I am… I couldn't afford to do that financially because the pay wasn't high enough. So I decided… I'd already got my own company, an engineering company, so the natural thing for me to do was to d my own thing and work independently. So, I set up a limited company, Blackst Forensics Limited, bought all my equipments through contacts in the industry. I started picking up work for police and law firms. Though [inaudible graduate, it's very difficult to start with...and work can be infrequent. We can get two or three jobs comes together, and then you make it looking for another month or two

B- Axial Coding:

Guidelines and procedure	Infrastructure	Organisation Polices	Human Resources (HR)	Investigation Process
- Make Sure you are able to acquire the potential evidence **(02CONINTUAE13)** - started Looking for a job and did not find suitable job then decided to have my own company (**01BLKINTUK13**)	- Forensic Lab Core module required (**02CONINTUAE13**) - field of forensic is an ocean because of technology **(02CONINTUAE13)** - I set up a limited company (**01BLKINTUK13**) - bought my equipment through contacts (**01BlkIntUK13**)		- studied forensic and security in the university, then disaster recovery, security, then external training and certification and more specialised training (**01BLKINTUK13)**	- Different types of investigation (**02CONINTUAE13**)

C- Selective Coding:

Theory on Guidelines and Procedures:

1- Ensuring that you are able to acquire the potential evidence used as a guideline for establishing a DFC

2- The process of establishing a company happened due not finding a suitable job

3- Education, training and certification was part of establishing the company

Theory on Infrastructure:

1 – The forensic lab is a core module in DFC

2- Because of the rapid evolution and huge production of new technology Forensics field become as an ocean.

APPENDIX 7: Establishing Tool Testing Capability Using DFOCC

1. Introduction:

Digital Forensics Organisation Core Capability (DFOCC) is a framework that aids Digital Forensics stakeholders to establish and manage their Digital Forensics Capability (DFC). The purpose of this experiment is to show a real application of DFOCC framework and DFOCC software. This includes an example of establishing a DFC using DFOCC framework and software. The researcher also uses DFOCC to allocate the right resources for establishing a tool testing capability. This is done by asking the user a number of questions related to each category.

First core capability is the Investigation which makes sure that all the details related to the investigation process is governed and documented, including Investigation process, Investigation procedure and Evidence admissibility. **Second** core capability is Infrastructure, which makes sure that those physical requirements for the specific capability are provided such as Tools, Building/Facility and the Virtual environment. **Third** core capability is People; this sets the criteria for assigning the right person, for specific task, equipped with knowledge, experience, education, training, organisation hierarchy and trait. **Finally** policy, this core category ensures that the previous core categories (Investigation, Infrastructure and People) are governed by policy.

The researcher aims to provide a road map for developers to establish digital forensics capabilities by applying DFOCC framework using the DFOCC software. This methodology consists of categories and subcategories very similar to the survey which allows allocating resources for DFC.

This chapter tests 3 functionalities of DF tools in 4 open source tools: Autopsy 4.1.0, Digital Forensics Framework 1.3.6-CE, ProDiscoverer 6.1.0.3 and OS Forensics 2.2 Build. The relationship among these mentioned tools is that they perform similar functionalities and that they are open source tools and compatible with windows operating system which are within the resources of the researcher. The test process will be in accordance to NIST

tool testing procedure (Active file Identification & deleted file recovery tool specification) (NIST, 2016). In the next section we will use DFOCC software in order to build the tool testing capability for this research.

2. Building to capability

At this stage the user is encouraged to use DFOCC software (Figure 1) to be able to allocate the resources needed for this capability. Building any capability according to DFOCC goes through four stages: Investigation, Infrastructure, People and Polices. In Each core category the user is asked a number of questions related to his needs to be considered and his answers and concerns are saved in a local database to be used in generating the capability report as shown in Figure 2.

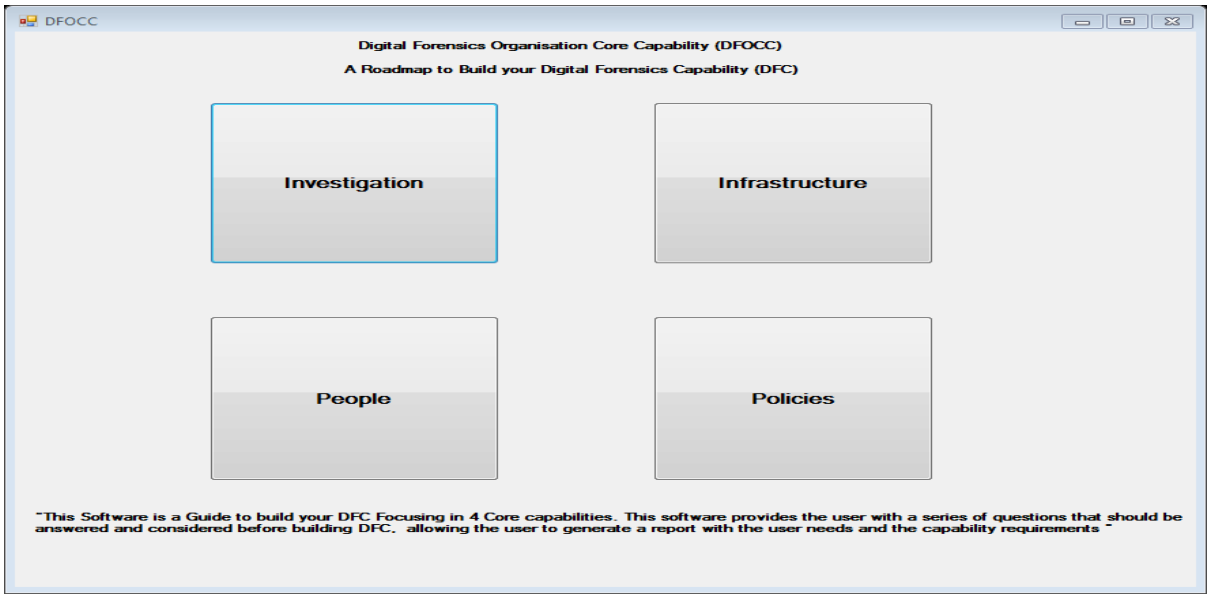


Figure 20 DFOCC Main Page

The report in figure 2 is generated from DFOCC. This report includes the user selection for his resources needed for the tools testing capability. In the Investigation category the user identified the purpose of this capability as tool testing and the scope of this experiment is to test 3 functionalities of 4 open source tools. The report shows the result of the user selection for the other categories as shown below in figure 2. After having a clear view of what is needed and a road map for building the tool testing capability, the researcher in the

next section starts his experiment by dividing the tool testing experiment into 3 tasks according to the functionality. **Task 1**: Identifying and recovering deleted files, **Task 2**: Testing File Carving using Digital Forensic Framework (DDF) and **Task 3**: String and File Name Search.

Investigation	Infrastructure
Investigation Process Purpose of Investigation --->Tool Testing --->Test 3 functionalties in 4 open source tools Analysis --->Viewing --->Navigating --->Examining --->Summary of Actions --->Documented Process --->NIST guidline for toold testing --->Expected Results Case Management --->Task Assigment Post-Investigation --->Publish Results --->compare results	Infrastructure Tools Tool Selection --->Software Forensic Analysis Software --->Autopsy,DFF,ProDiscoverer and OSForensics Building a Facility Functionality and Scope --->Research and Development Facility Requirements --->Ofice Space --->PC
People	**Policies**
People Knowledge Information Technology --->-University degree General Forensics --->-Digital Forensics Specialised Skills --->-Require special skill for a task Education Type od Disciplines --->-Computer science Quality of Degree --->-Academic Length of Experience --->-Fresh graduates Training and Development Types of Training --->-Self-education Organisation Hierarchy Management Levels --->Academic Size of Organisation --->One person ---------- ---------- Type of Organisation --->-Academic	Policies Building and Management Standards --->- ISO Key Success Factors --->-Use of Standards Confidentiality and Non-Disclosure --->De Montfort University Ethical Approval

Table 21 Report Generated from DFOCC for Building the Capability

3. Task 1: Test the functionality of (identifying and recovering deleted files) in 4 tools

In this section the researcher will test the functionality: identifying and recovering deleted files in 4 tools. This test will be according to NIST guideline for testing tools.

3.1 Test Requirements

NIST identified four requirements for the tool:

A) To be capable of recovering and viewing deleted files according to NIST (2014) the tool should be able to perform as below:

1. *"The tool shall identify all deleted File System-Object entries accessible in residual metadata.*
2. *The tool shall construct a Recovered Object for each deleted File System- Object entry accessible in residual metadata.*
3. *Each Recovered Object shall include all non-allocated data blocks identified in a residual metadata entry.*
4. *Each Recovered Object shall consist only of data blocks from the Deleted Block Pool". (NIST, 2014)*

3.2 Test Assertion

Is the tool able to recover the deleted files from the known file systems, FAT32 and NTFS, with their corresponding metadata using Autopsy 4.1.?

3.3 Test Methodology:

- Forensic Tool: Autopsy 4.1
- Digital Forensics Framework 1.3.6-CE
- ProDiscoverer 6.1.0.3
- OS Forensics 2.2 Build free version
- Operating system: Windows 7 Enterprise 64-bit; RAM: 4GB

3.4 Procedure Steps:

1. A USB drive (AUTOPSYTEST) is first formatted in the FAT32 file format to use it as test image in the experiment because the NIST did not provide test images for testing recovery of deleted files therefore the researcher took this initiative.

2. 5 new files have been added to the USB drive namely:

    - 1.txt

- 2.txt
- 3.jpg
- 4.jpg
- 5.doc

3. Three files were deleted:
    - 1.txt
    - 3.jpg
    - 5.docx

4. A forensic image of the USB drive made using (AccessData® FTK® Imager 3.2.0.3).

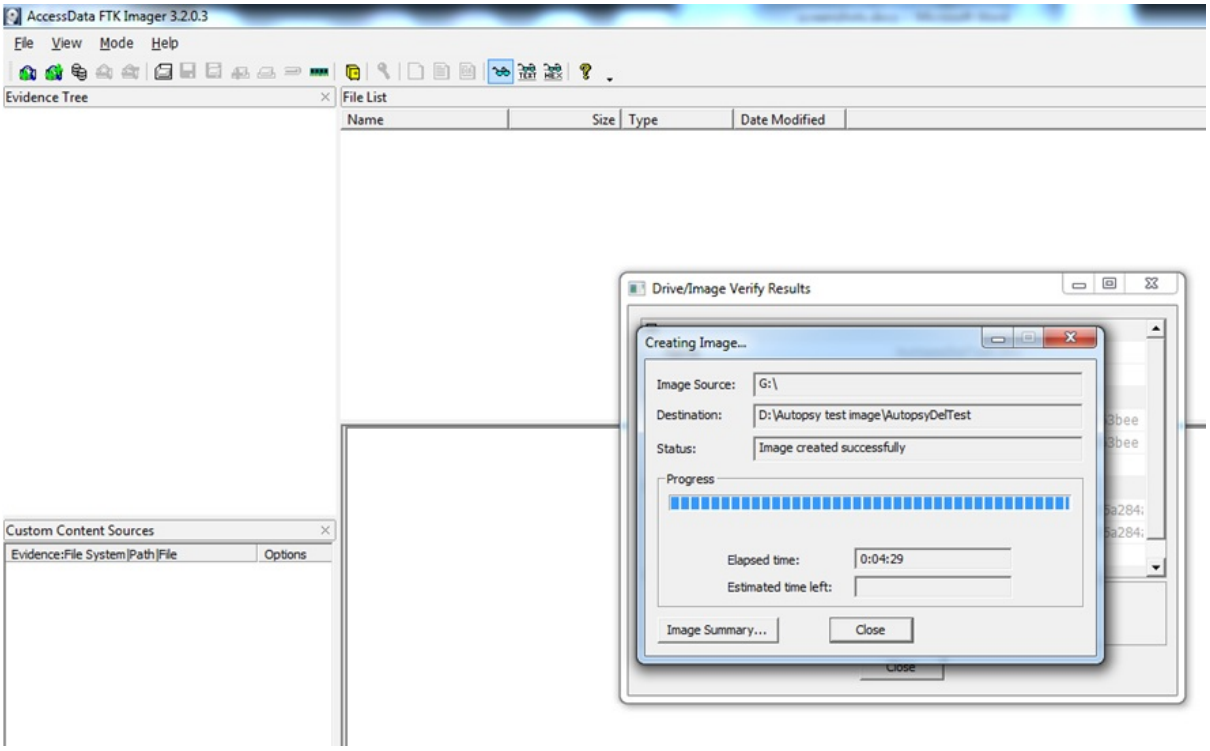


Table 22 Creating USB Image

5. The image file added to Autopsy 4.1 Forensic software.

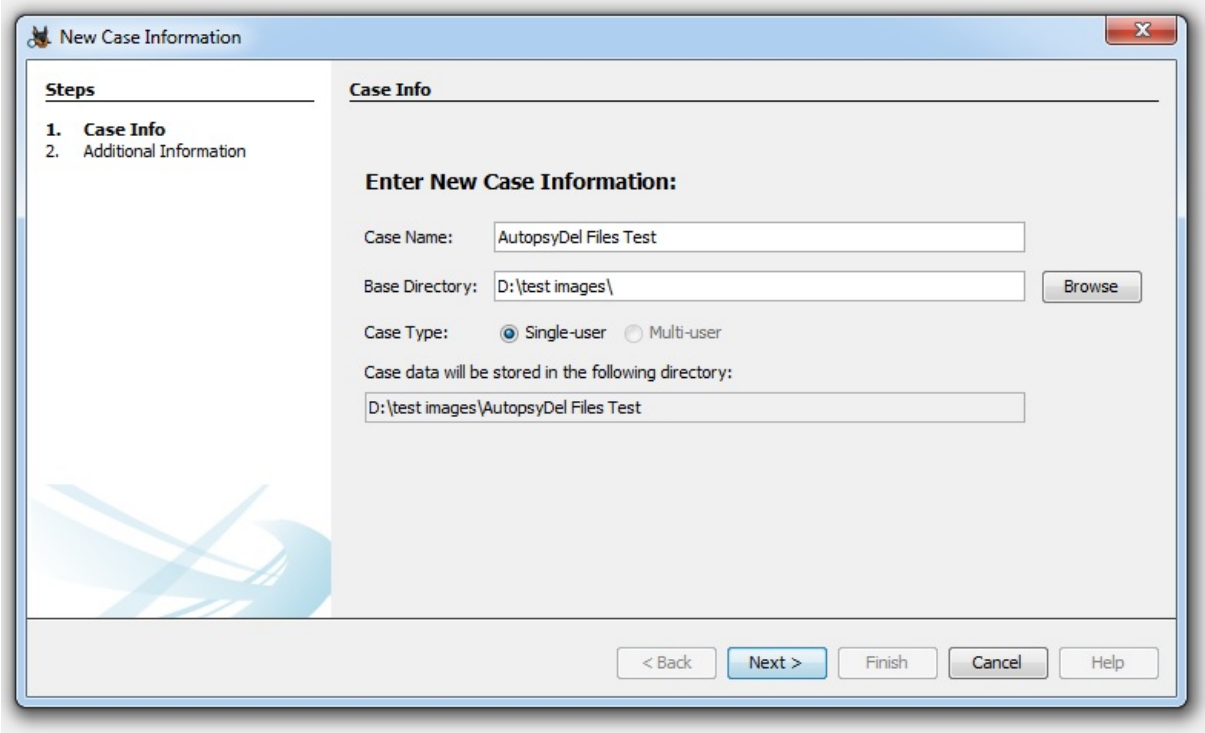


Table 23 creating the case

6. The image file examined to check whether the deleted files show up in the list along with the file names and their extensions.

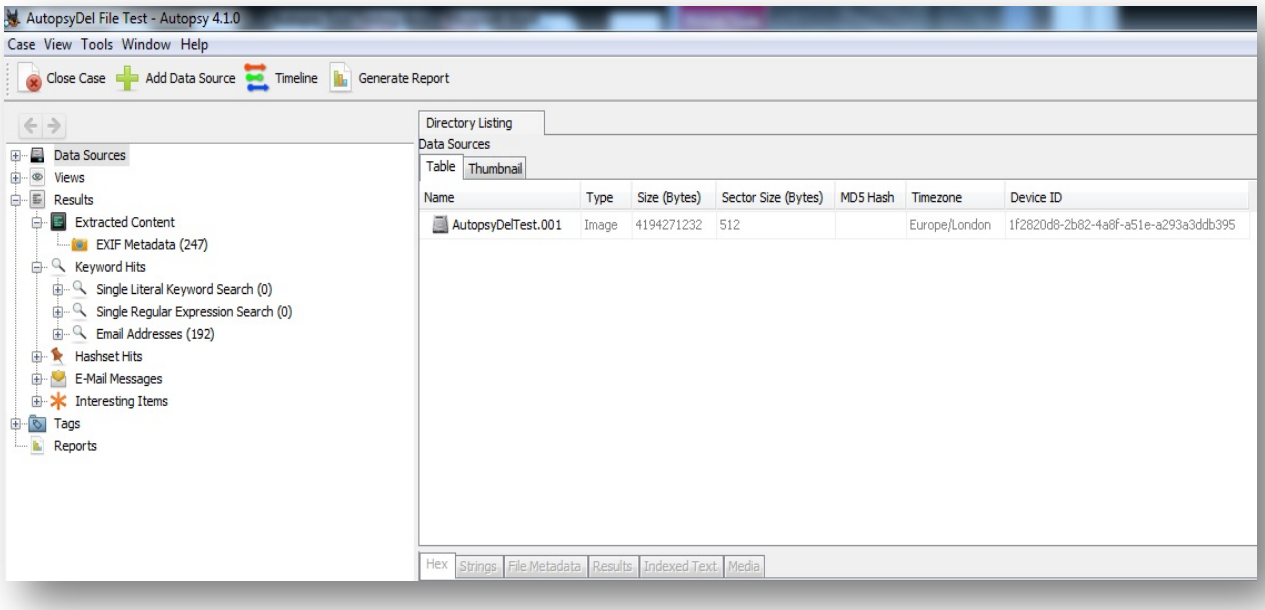


Table 24 Examine Test Image

7. The content of the deleted files checked to see whether the forensic tool recovers the deleted files completely.

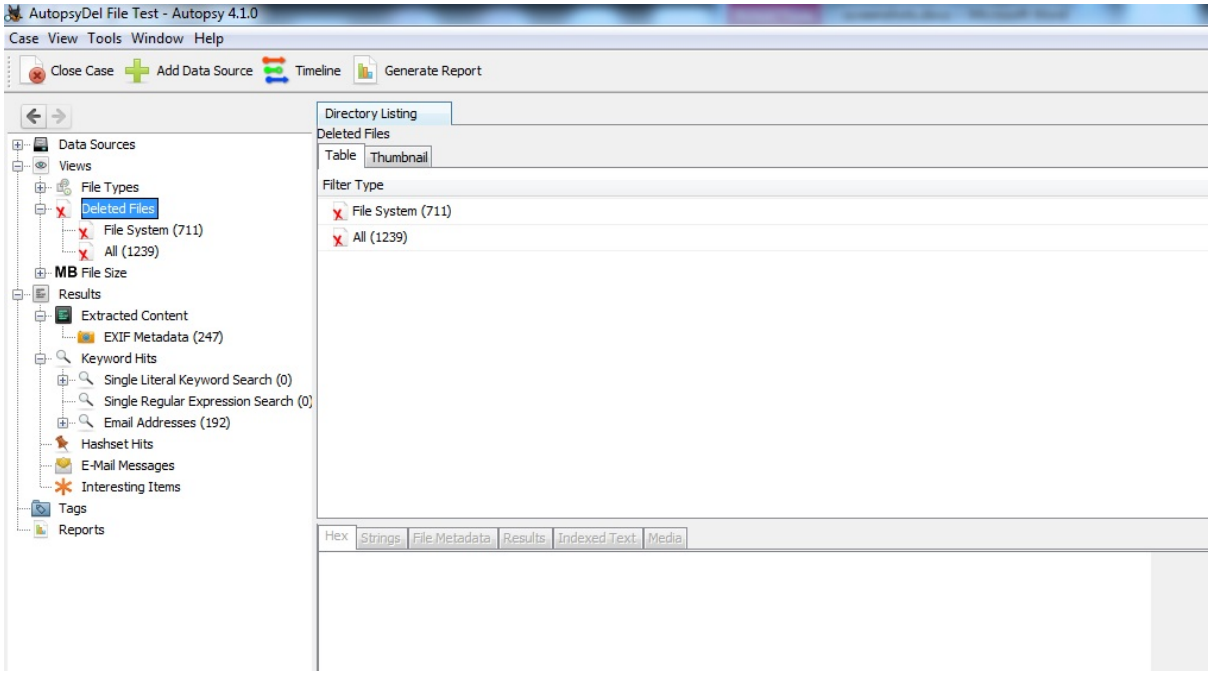


Table 25 exploring the content of the test image

8. The deleted file metadata such as File Creation, Modification, and Accessed times checked against the forensic tool.

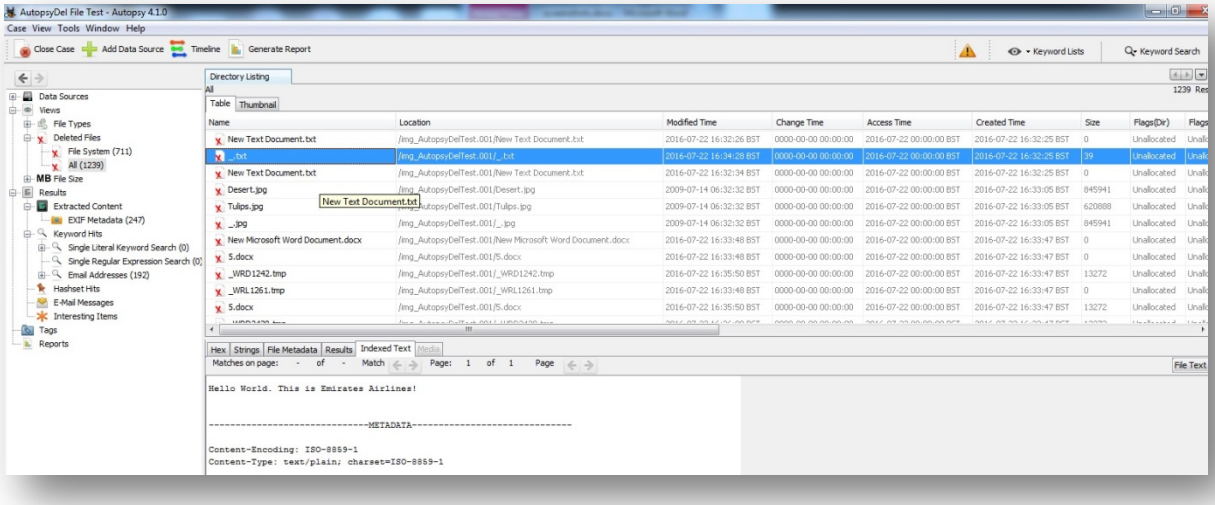


Table 26 Viewing metadata

3.5 Test Results:

All tools were able to retrieve the deleted items; however they vary in the way user can examine the deleted items and the representation of the data itself. Test results for the 4 tools are presented in details in section 6.

4. Task 2: Testing File Carving using Digital Forensic Framework (DDF)

4.1 Test Requirements

According to NIST standard in order to certify a computer forensic to be capable of file carving, the tool has to be able to satisfy the following mandatory requirements:

All file carving tools must support the following requirements.

- *"The tool shall return one carved file for each supported file header signature from a source file that is present in the search arena.*
- *A carved file shall only contain data blocks from the search arena.*
- *All data blocks in a carved file shall originate in a single source file.*
- *The file type of a carved file shall match the file type of its contents.*
- *The tool shall return carved files in a state that conforms to a valid file of the carved file type".(NIST, 2014)*

This experiment tests DFF version 1.3.6-CE using NIST standard, and the result is based on the Graphic File Carving Report (Test Results for Graphic File Carving Tool:FTKv4.1, 2014). The reason for choosing this tool in this test is because the test images available were not recognised by any of the other tools used in this experiment therefore it was appropriate to conduct the investigation with only one tool for this specific functionality.

4.2 Test Results for Graphic File Carving Tool

Tool Tested: Digital Forensic Framework (DFF)

Software Version: v1.3.6-CE

Supplier: ArxSys

Website: http://www.arxsys.fr/

4.3 Test Case Selections

The ability of DFF v1.3.6-CE ability to carve graphics gif, bmp, png, jpg, tiff files was measured by analysing carved graphics files from raw disembodied "dd" images (i.e., an image without a filesystem) which contain various layouts of fragmentation and completeness. The dd image layouts are:

- ***"No Padding:*** *contiguous files with no other content between files*
- ***Cluster Padded****: contiguous files with assorted levels of content ranging in size from 1, 2, 4, 8, 16, …128 sectors*
- ***Fragmented In Order****: contiguous and sequential fragmented files with content separating the files*
- ***Incomplete:*** *contiguous and partial (i.e., only a portion of the file is present) files*
- ***Fragmented Out of Order:*** *contiguous and disordered fragmented files separated by other content*
- ***Braided Pair:*** *contiguous and intertwined fragmented files*
- ***Byte Shifted:*** *contiguous files that are not aligned to sector boundaries" (NIST,2014)*

4.4 Testing Environment

The tests were run in the DMU Research lab GH6.12. This section describes the selected test execution environment.

4.4.1 Execution Environment

DFF version 1.3.6-CE was installed on Windows 7 Enterprise SP 1.

4.5 File Carving Test Results

The table below contains 6 columns and 6 rows. The columns contain total number of files carved and whether the carved files were Viewable - Complete/minor alteration; Viewable – Incomplete/major alteration; Not Viewable or a False Positive.

> *"The Total Carved column reports the total number of files carved. This number is often higher than the number of files contained within the image. This is generally*

due to false positives. False positives often occur when a tool has carved a file based upon a known file signature (e.g., FF D8) string that is not a file header, but a string within another file.

The Viewable – Complete/minor alteration column describes carved files in which the picture appears to be unchanged from the original or the changes are so minor that the full content, colour, and other attributes of the picture are maintained.

The Viewable – Incomplete/major alteration column include partial recoveries (i.e., only parts of the graphic are viewable), scrambled pictures in which the fragments are assembled incorrectly, colour shifts and similar changes.

The Not Viewable column describes a file that is not viewable, could not be opened or had no content when opened."(NIST, 2014)

4.5.1 Fragmented In Order

In this section the DFF tool is tested for its analysing capability when the graphic files are contiguous and are sequentially fragmented with content in between the files. The image file used here was L1_Graphic.dd, shown in the table below:

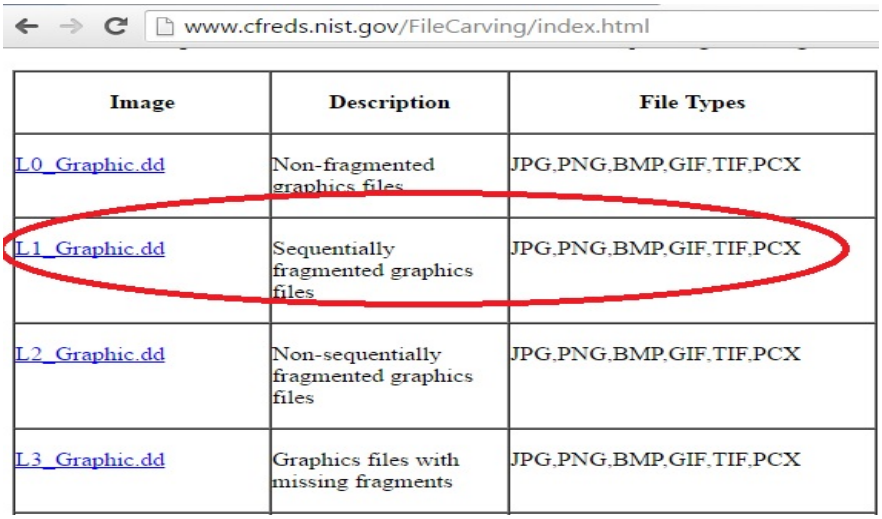


Image	Description	File Types
L0_Graphic.dd	Non-fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX
L1_Graphic.dd	Sequentially fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX
L2_Graphic.dd	Non-sequentially fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX
L3_Graphic.dd	Graphics files with missing fragments	JPG,PNG,BMP,GIF,TIF,PCX

Table 27 L1_Graphic.dd Image File

Test Name: Fragmented In	Total Carved	Viewable Complete	Viewable Incomplete	Not Viewable	False Positive

Order					
Files	2659				
1 gif					
Contiguous	1		1		
Frag w/Fill	0				
80 jpg					
Contiguous	2	1	1		
Frag w/Fill	78			78	
2571 bmp					
Contiguous	1		1		
Frag w/Fill	2570			2570	
1 tif					
Contiguous	0				
Frag w/Fill	1			1	
1 png					
Contiguous	1	1			
Frag w/Fill	0				

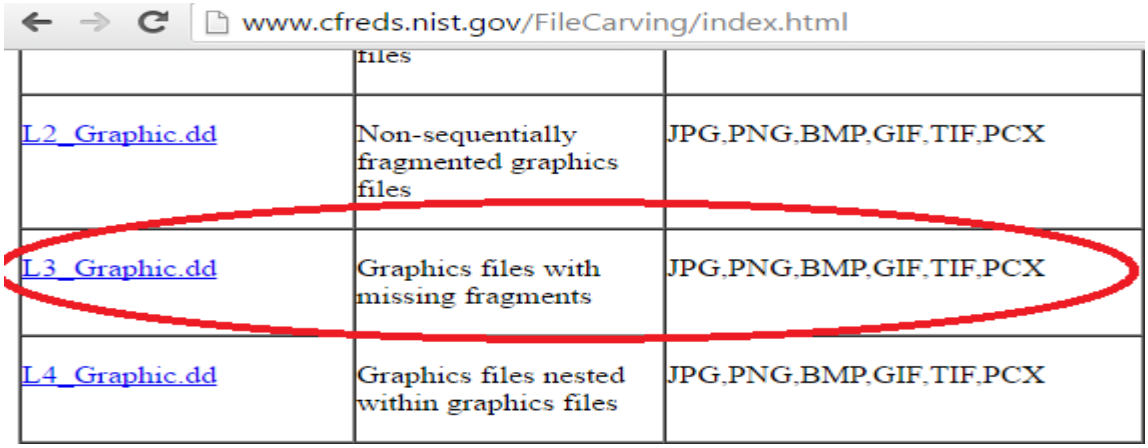
Table 28 Fragmented In Order

The Table 9 presents the result of analysing L1_Graphic.dd (NIST Test Images, 2016) file which is used as test image.

- This contains a total of 2659 files, 5 of which are contiguous and 2654 that are sequentially fragmented with filler that ranges in size from 1, 2, 4, 8, …128 sectors.
- Out of the 2659 files carved 1 was gif, 80 were jpg, 2571 bmp, 1 tif, and 1 png graphic file.
- 2 Files were viewable fully, 3 files Viewable incomplete, and 2649 files were not viewable at all.

4.5.2 Incomplete

In this section the DFF tool is tested for its analysing capability when the graphic files are contiguous and are partial. The image file used here was L3_Graphic.dd shown in the table below:



	files	
L2_Graphic.dd	Non-sequentially fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX
L3_Graphic.dd	Graphics files with missing fragments	JPG,PNG,BMP,GIF,TIF,PCX
L4_Graphic.dd	Graphics files nested within graphics files	JPG,PNG,BMP,GIF,TIF,PCX

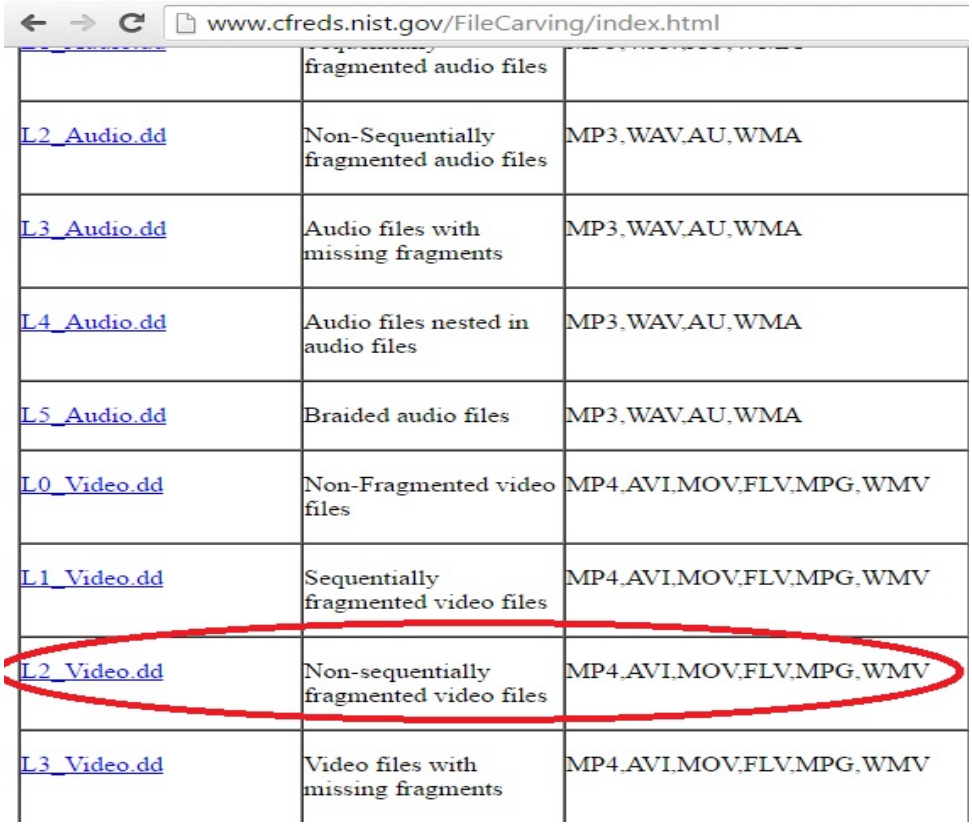
Table 29 L3_Graphic.dd Image File

Test Name: Incomplete	Total Carved	Viewable Complete	Viewable Incomplete	Not Viewable	False Positive
Files	1434				
77 jpg					
Complete		1		1	
Partial					
1353 bmp				1353	
Complete					
Partial					
1 tif					
Complete				1	
Partial					

Table 30 Incomplete

4.5.3 Fragmented Out of Order

In this section the DFF tool is tested for its analysing capability when the video files are contiguous and are not sequentially fragmented. The image file used here was L2_Video.dd shown in the table below:



	fragmented audio files	
L2_Audio.dd	Non-Sequentially fragmented audio files	MP3,WAV,AU,WMA
L3_Audio.dd	Audio files with missing fragments	MP3,WAV,AU,WMA
L4_Audio.dd	Audio files nested in audio files	MP3,WAV,AU,WMA
L5_Audio.dd	Braided audio files	MP3,WAV,AU,WMA
L0_Video.dd	Non-Fragmented video files	MP4,AVI,MOV,FLV,MPG,WMV
L1_Video.dd	Sequentially fragmented video files	MP4,AVI,MOV,FLV,MPG,WMV
L2_Video.dd	Non-sequentially fragmented video files	MP4,AVI,MOV,FLV,MPG,WMV
L3_Video.dd	Video files with missing fragments	MP4,AVI,MOV,FLV,MPG,WMV

Table 31 L2_Video.dd Image File

Test Name: Fragmented Out of Order	Total Carved	Viewable Complete	Viewable Incomplete	Not Viewable	False Positive
Files	2659				
avi	1	1			
mov	2			2	

mov	**3**			**3**	
mov	**3**			**3**	
wav	**1**		**1**		
mpg	**11028**	**> 1000**			
mpg	**41**	**39**		**2**	

Table 32 Fragmented out of order

4.5.4 Braided Pair

In this section the DFF tool is tested for its analysing capability when the graphic files are contiguous and are intertwined fragmented. The image file used here was L5_Graphic.dd shown in the table below:

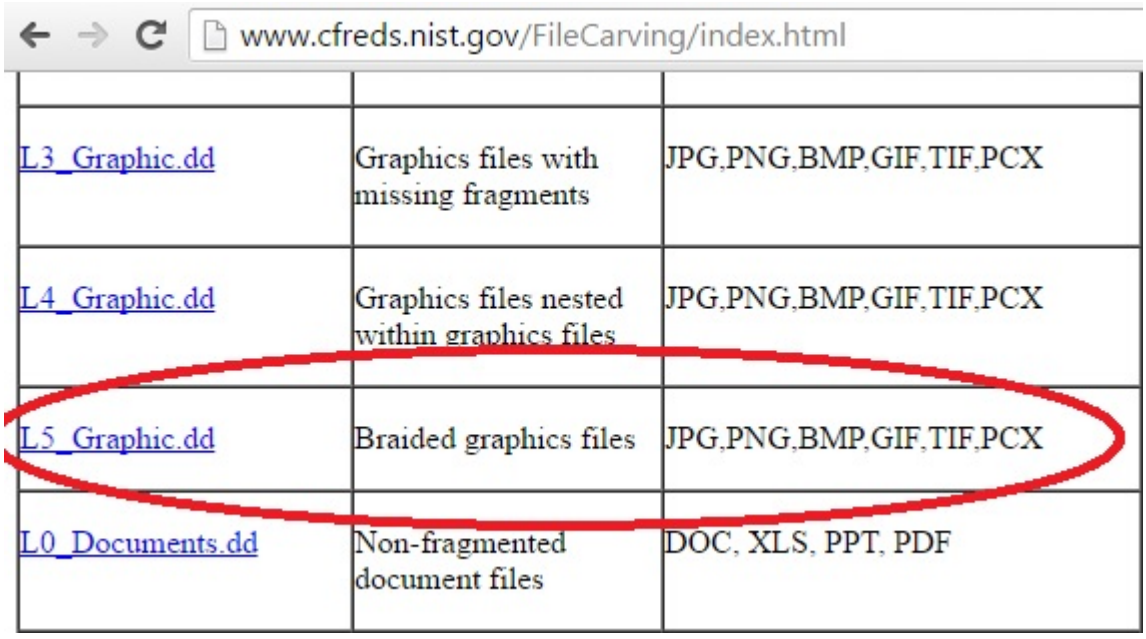


Table 33 L5-Graphic.dd Image File

Test Name: Fragmented In Order	Total Carved	Viewable Complete	Viewable Incomplete	Not Viewable	False Positives
Files	2697				
1 gif					
Contiguous	1		1		
Braided	0				
80 jpg					
Contiguous	2	1	1		
Braided	78			78	
2571 bmp					
Contiguous	1		1		
Braided	2609			2609	
1 tif					
Contiguous	0				

Braided	**1**			**1**	
1 png					
Contiguous	**1**	**1**			
Braided	**0**				

Table 34 Braided Pair

4.5.5 No Padding

In this section the DFF tool is tested for its analysing capability when the graphic files are contiguous and with no contents in between the files. The image file used here was L0_Graphic.dd shown in the table below:

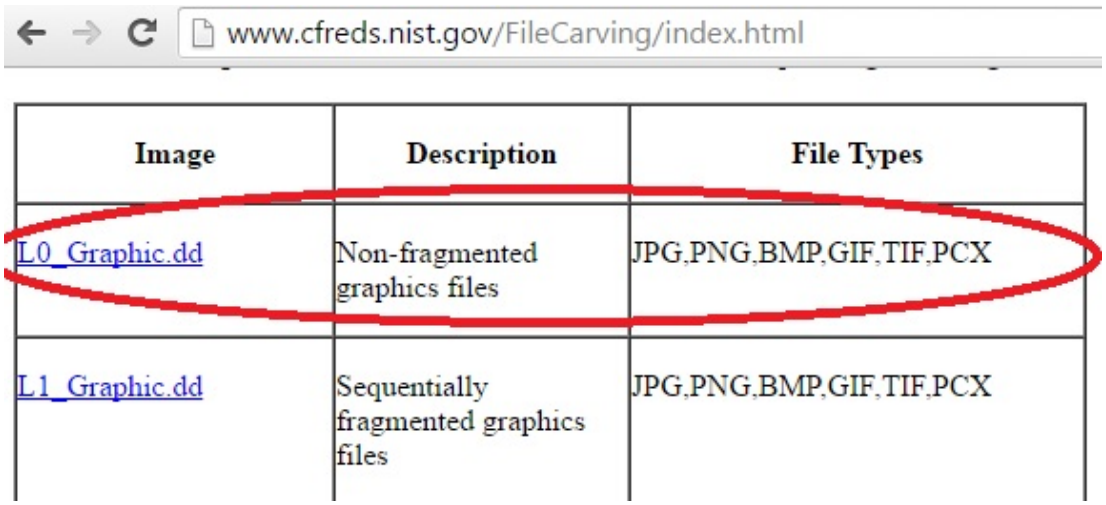


Image	Description	File Types
L0_Graphic.dd	Non-fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX
L1_Graphic.dd	Sequentially fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX

Table 35 L0_Graphic.dd Image File

Test Name: Fragmented In Order	Total Carved	Viewable Complete	Viewable Incomplete	Not Viewable	False Positive
Files	**2659**				
gif	**1**		**1**		
jpg	**80**				

bmp	**2571**	**1**		**2570**	
tif	**1**			**1**	
png	**1**			**1**	

Table 36 No Padding

4.6 File Carving Results Summary

DFF 1.3.6-CE was mostly successful at carving mpg files across all test images in a viewable state. The majority of carved bmp files were not viewable. It does not carve tiff files. Generally, no more than 1 tiff or gif file per test image is carved in a complete or viewable state.

5. Task 3: String and File Name Search

5.1 Test Requirements:

In this task open source tools (Autopsy, DFF, ProDiscoverer and OS Forensics) tested for string and file name Search functionality. According to NIST, (2014) testing string search functionality in digital forensics tool should meet number of requirements (Mandatory and optional) to fulfil in order to be able to string and file name search. This test considers only mandatory requirements. Below the tables are presented mandatory requirements for a tool.

- "The response returned by a query is equal to the match set for the query.
- The tool shall search using one or more specified character representations"(NIST,2014)

5.2 Test Assertion

Are tools able to perform a string and file name search. Also are these tools able to perform search in the delete files from the known file systems, FAT32 and NTFS.

5.3 Test Methodology:

Tools used:

- Forensic Tool: Autopsy 4.1

- Digital Forensics Framework 1.3.6-CE

- ProDiscoverer 6.1.0.3

- OS Forensics 2.2 Build free version

- Operating system: Windows 7 Enterprise 64-bit; RAM: 4GB

5.4 Procedure Steps:

A USB drive (AUTOPSYTEST) is first formatted in the FAT32 file format to use it as test image in the experiment because NIST did not provide test images for testing recovery with published reports therefore we had to create a test image for this purpose.

The USB drive (AUTOPSYTEST) same image file, used in task 1, was added to Autopsy 4.1 Forensic software, Digital Forensics Framework 1.3.6-CE, ProDiscoverer 6.1.0.3 and OS Forensics 2.2 Build free version. Below is a screen shot from Autopsy string and file name search.

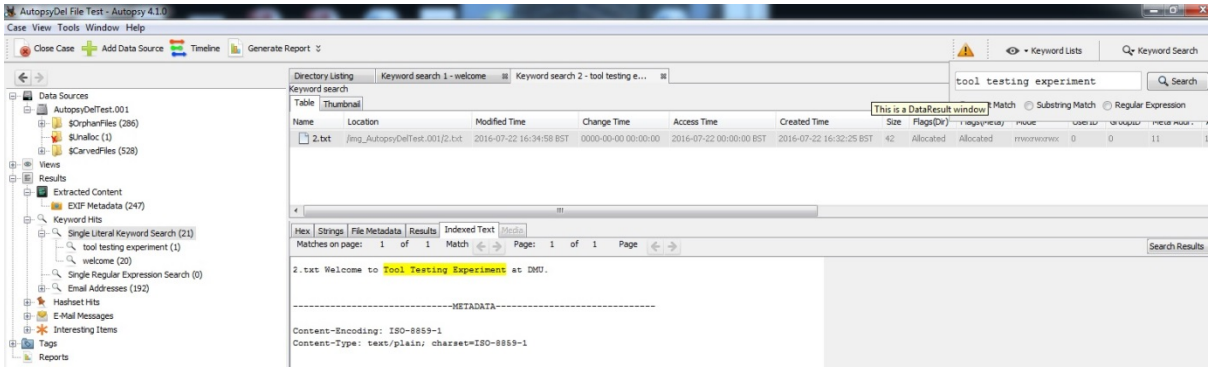


Table 37 Running String Search in Autopsy

5.5 Test Results:

All tools were able to retrieve string and file names; however, they vary in the ease of use in each tool. For example, Autopsy searches for string and file name in the whole drive,

however, some other tools the user needs to specify a specific file in order to perform a string search. In the next section a detailed test results are presented in table 19.

6. Conclusion:

In this section all the test results from previous tasks are presented in Table 19 below. The purpose of this experiment is to use DFOCC framework and DFOCC software in real life. Both the framework and the software facilitated the process of establishing this capability (DF Tool Testing Capability). The reason behind that is because the DFOCC provided the roadmap. The methodology used in this test was NIST methodology for tool testing and all procedures were in accordance with NIST tool testing guideline. All test results are grouped in the table below to provide a summary of the tools and functionality tested. Finally, this is an experiment for research purposes and results shown in table 19 do not aim to provide a base for any criticism or index for the performance of the any tool used.

Functionality	Autopsy	Digital Forensic Framework (DFF)	ProDiscoverer	OS Forensics
Deleted Files Recovery	The deleted files 1.txt, 3.jpg, and 5.docx were: 1-identified by Autopsy 4.1.0 2- Recovered along with their content. 3- Placed in an ascending order in the list. 4- The files which were renamed were also being identified as deleted files.	1-DFF identified the deleted items 2-The deleted files were recovered along with their content 3-Some of the files that are recovered has been renamed by DFF	1- identified the deleted items 2-The deleted files were recovered along with their content	1- identified the deleted items 2-The deleted files were recovered along with their content

	5- The Modified, Accessed, and Created times are shown by the Autopsy 4.1.0 forensic software.			
Forensic File Carving	Test Images provided NIST website was undefined file system and therefore Autopsy was not able to read the test Image used in the NIST website.	-DFF 1.3.6-CE was mostly successful at carving **mpg** files across all test images in a viewable state. -The majority of carved **bmp** files were not viewable. - It does not carve **tiff** files. Generally, no more than 1 **tiff** or **gif** file per test image is carved in a complete or viewable state.	Test Images provided NIST website was undefined file system and therefore ProDiscovere was not able to read the test Image used in the NIST website.	Test Images provided NIST website was undefined file system and therefore Forensics was not able to read the test Image used in the NIST website.
String Search	Able to retrieve the text and file which was used in the test in a file(file name search and content search)	-Able to Search for file names and deleted files name	Able to Search for file names and content of the files directly	-Is able to search for file names and deleted files name - Is not able to search for the content direct however you need to do content search for every file individually

Table 38 General Test Results

References:

1. NIST, 2014Test Results for Graphic File Carving Tool: FTKv4.1 Available on:

https://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_FTK%20v4.1%20Test_%20August%202015_Final.pdf . Accessed on: 27/07/2016

2. NIST, 2014 Forensic File Carving Tool Specification 7 8 9 Draft Version 1.0 for Public Comment. Available on: http://www.cftt.nist.gov/FC-req-public-draft-01-of-ver-01.pdf. Accessed on: 26/07/2016

3. (NIST Test Images, 2016) Available on: http://www.cfreds.nist.gov/FileCarving/index.html Accessed on: 27/07/2016

APPENDIX 8: Formulating Interview Questions

Aims	Objectives	Questions
1-Identify , document, evaluate the stages and the procedures followed by organizations in the development of their Forensic Capacity	1- Identify and evaluate the existing recommendation regarding developing a Digital Forensic Provision by studying at least 3 examples	a- What recommendation exists in literature regarding developing F P? b- If recommendation is available how widely they are used? c- How effective they are?
2- Propose a development framework for those starting the development of their own Forensic Capacity	2- discover and document how range of organizations develop their own forensic capacity by studying at least 3 different types of organizations in different countries	a- How did range of organizations develop their Forensic Capacity? b- What guidance did organizations used to develop their F C? c- What challenges faced by organizations in developing their F P?
	3- identify the extent to which "best practice "in developing Digital Forensic Capacity exist by finding how widely they are used and the success rate in cases	a- Is there a standard pattern identifiable in developing DFC? b- What is the role of international and national bodies in developing DFC?
	4- evaluate the impact of organizational , cultural influences in developing forensic provision and its implementation by providing no less than 3 examples of the influences and their impact	a- What influence do organizational social and professional procedures do have on the development of DFC? b- How do personnel in forensic professionals manage and recognize pressure from various stakeholders on their professional practice?
	5- to document the range of tools used in the variety of organizations and how the choice is made for their use by studying at least 5 different tools used in different organizations	a- How do organizations select and validate their tools? b- What tools are used? c- How effective they are? d- How can Forensic Provision improve tools?
	6- identify and document the training requirement for different forensic practitioners in a range of organizations and particularly in regard to CPD (Continuing Professional Development) by examining training in at least 3 different organizations	a- How training needs are identified? b- How training needs are met? c- What qualifications are looked in the forensic professional? d- How effective are professional bodies and training organizations in providing forensic professionals?
	7- map the current provision of Digital Forensic in range of organizations and cultures by viewing at least 3 different organizational structures	a- What is the structure for Digital Forensic provision in a range of organizations and cultures?

Interview Questions (IQ)	Research Aims		Research Questions (RQ)					
	Aim 1	Aim 2	RQ1(G)	RQ2(G)	RQ3(HR)	RQ4(HR)	RQ5(Infrastructure)	RQ6(IP)
IQ1	●			●				
IQ2	●			●				
IQ3	●			●				
IQ4	●			●				
IQ5	●			●				
IQ6		●						
IQ7							●	
IQ8		●						
IQ9	●		●					
IQ10				●				
IQ11	●							
IQ12	●						●	
IQ13	●						●	
IQ14	●		●				●	●
IQ15	●				●			●
IQ16	●							●
IQ17		●						●
IQ18		●						●
IQ19	●						●	
IQ20	●				●			
IQ21	●						●	
IQ22	●					●		
IQ23	●					●		
IQ24		●				●		
IQ25	●							●
IQ26	●						●	
IQ27		●						●
IQ28	●						●	
IQ29		●						●